PRIVACY INTERNATIONAL

Stakeholder Report
Universal Periodic Review
31st Session - Jordan

The Right to Privacy in the Hashemite Kingdom of Jordan

Submitted by Jordan Open Source Association (JOSA) and Privacy International

March 2018

The Right to Privacy in the Hashemite Kingdom of Jordan

March 2018

PRIVACY INTERNATIONAL

www.privacyinternational.org

Jordan Open Source Association

Introduction

1. This stakeholder report is a submission by Privacy International (PI) and the Jordan Open Source Association (JOSA). PI is a human rights organisation that works to advance and promote the right to privacy and fight surveillance around the world. Jordan Open Source Association (JOSA) is a Jordanian non-profit organization that works to promote Open Source, Free Culture and Digital Rights, including the Right to Privacy and the protection of the personal data of Jordanian citizens.

2. Privacy International and the Jordan Open Source Association wish to bring concerns about the protection and promotion of the right to privacy for consideration in Jordan's upcoming review at the 31st session of the Working Group on the Universal Periodic Review.

Follow Up to the Previous UPR

3. In Jordan's previous reviews, no express mention was made of the right to privacy in the context of data protection and communications surveillance in the National Report submitted by Jordan or the report of the Working Group.

4. However, concerns were expressed in a stakeholder submission regarding the crackdown on online activities of users and the policy of the Ministry of the Interior which required owners of Internet cafes to provide information on users and to prevent access to specified websites were expressed by stakeholders.[1]

5. Jordan also received recommendations on ensuring freedom of Internet media and removing requirement to register independent Internet sites.[2]

Domestic Laws Related to Privacy

6. The Constitution of Jordan[3] contains several provisions on the right to privacy:

   Article 7:

   1) Personal freedom shall be guaranteed.

   2) Every infringement on rights and public freedoms or the inviolability of the private life of Jordanians is a crime punishable by law.

   Article 18:

   "All postal and telegraphic correspondence, telephonic communications, and the other communications means shall be regarded as secret and shall not be subject to censorship, viewing, suspension or confiscation except by a judicial order in accordance with the provisions of the law."

[1] A/HRC/WG.6/17/JOR/3, para 62, pp 9. Available at: http://www.ohchr.org/EN/HRBodies/UPR/Pages/JOIndex.aspx

[2] A/HRC/25/9. Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G14/100/63/PDF/G1410063.pdf?OpenElement

[3] Available at: in English at: http://cco.gov.jo/Portals/0/constitution_en.pdf

7. The Telecommunications Law (13/1995) also states in Article 56:[4]

"Telephone calls and private Telecommunications shall be considered confidential matters which may not be violated, under legal liability."

International Obligations

8. Jordan has ratified the International Covenant on Civil and Political Rights (ICCPR)[5] and the Convention on the Rights of the Child (ratified November 1990), which both uphold the right to privacy. Furthermore, Jordan has signed Cairo Declaration on Human Rights in Islam (signed August 1990)[6] which also upholds the right to privacy.[7]

AREAS OF CONCERN

I. Communications Surveillance

9. Since early 2010, reports have emerged of increased reliance on surveillance, including to repress dissent, as more charges derived from surveillance are being pressed against activists.[8]

10. Despite growing concerns raised by civil society organisations in relation to the right to privacy in Jordan, there is very little independent, publicly scrutiny of policy and legislative processes on privacy, data protection and communications surveillance, and very limited reports on the surveillance powers and practices of Jordanian authorities.[9]

Absence of Legal Framework

11. There are some laws regulating communications surveillance as well as

[4] English language version available at: https://ppp.worldbank.org/public-private-partnership/sites/ppp.worldbank.org/files/documents/Jordan_telecomunication%20law_1995_EN.pdf

[5] Article 17 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 party 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]."

[6] Article 16 provides that, "1) No child 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. 2) The child has the right to the protection of the law against such interference or attacks."

[7] Article 18 provides that, "a) Everyone shall have the right to live in security for himself, his religion, his dependents, his honor and his property. (b) Everyone shall have the right to privacy in the conduct of his private affairs, in his home, among his family, with regard to his property and his relationships. It is not permitted to spy on him, to place him under surveillance or to besmirch his good name. The State shall protect him from arbitrary interference. (c) A private residence is inviolable in all cases. It will not be entered without permission from its inhabitants or in any unlawful manner, nor shall it be demolished or confiscated and its dwellers evicted."

[8] See: 7iber, 3 November 2013. Available: https://www.7iber.com/2013/11/state-security-court-2/#.V-p0TGWtGT9; Shukkeir, Y.,Confiscating the carrier pigeon: Jordan's response to online surveillance, AlarabAlyawm, GISWatch, Communication surveillance in the digital age. Available at: https://giswatch.org/en/country-report/communications-surveillance/jordan

[9] See: 7iberInformationandtheResearchCenteroftheKingHusseinFoundation(IRCKHF) (2015)A Glimpse into the perception of digital privacy in Jordan, Available at: https://www.7iber.com/research/a-glimpse-into-the-perception-of-digital-privacy-in-jordan/

regulations which impose obligations on service providers to enable and/or conduct themselves communications surveillance activities. However, when it comes to digital communications, there are no laws regulating their access by law enforcement and intelligence agencies.[10]

12. The Anti-Terrorism Law of 2006 lacks many substantive and procedural safeguards needed to ensure any interference with privacy is lawful, necessary and proportionate.

    - The law authorises the general prosecutor to subject someone to surveillance based on "reliable" information that links that person to "terrorist activities" without any clear language prescribing what "reliable" or "activity" means. Its article 4 states: "If the Prosecutor General received reliable information indicating that a person or group of persons is connected to any terrorist activity, the Prosecutor General can impose surveillance over the residence of the suspect, their movements, and their means of communication.
    - This weak threshold ("reliable information") fall short of the standard of "reasonable suspicion" set by human rights law and it provides too broad a discretion to allow for the request of a warrant.[11]
    - On the procedural side, according with Article 4(a) the general prosecutor can impose surveillance over a suspect's residence, their movements and means of communication for up to a month, search the place where a suspect is present, and confiscate anything connected to terrorist activity.[12] In case of complaints, the competent tribunal is the State Security Court (SSC), a special tribunal derived from military courts that can also rule over civilians.[13] The extension of the prosecution powers and the powers of the SSC fall short of the necessity and proportionality needed to incur in any affectation of human rights, and in particular the right to privacy.[14]

13. In 2015, the Cyber Crime Law was implemented. It allows *"employees of judicial authorities, upon receiving permission from the specialised prosecutor or court, to enter any location suspect of being used to commit any of the crimes stated in this law. They are also permitted to search devices, tools, programmes, operating systems, and the web (servers) which are suspected of being used to commit any of said crimes."*[15]

[10] See: Internet Legislation Atlas, Jordan: Surveillance and data protection, available at: https://internetlegislationatlas.org/#/countries/Jordan/frameworks/surveillance

[11] See: Privacy International and 7iber, State of Privacy – Jordan. Last updated in January 2018, available at: https://privacyinternational.org/state-privacy/1004/state-privacy-jordan; Jordan – Regulation of Online Content, Internet Legislation Atlas, available at: https://internetlegislationatlas.org/#/countries/Jordan/frameworks/content-regulation

[12] Anti-Terrorism Law No. 55 of 2006, available at: https://ihl-databases.icrc.org/applic/ihl/ihl-nat.nsf/0/4d39e76935f76f4fc125767e00320698/$FILE/Anti-Terrorism%20Law.PDF

[13] For further information visit: The Hashemite Kingdom of Jordan, Government – The Judicial Branch, available at: http://www.kinghussein.gov.jo/government4.html

[14] See: Gulf News, Amnesty urges Amman to amend or repeal the anti-terrorism law, 10 November 2016, available at: http://gulfnews.com/news/mena/jordan/amnesty-urges-amman-to-amend-or-repeal-anti-terrorism-law-1.265118

[15] Al masri, R., Cybercrime Law – How does the government control the online platform?, 7iber, 30 January 2018, available at: https://www.7iber.com/technology/cyber-crime-law-how-does-the-government-control-the-online-platform/

14. The government has proposed a Cybercrime Bill Amendment Draft,[16] which is waiting to be discussed by the Parliament. The proposed amendments would give more authority to the prosecutor. As reported by 7iber, *"the proposed amendment includes adding the word 'search' after 'enter' in the previous text in order to widen the scope of 'locations' that can be searched (devices, applications, and homes). It also includes giving more authority to the prosecutor, allowing them to confiscate devices and tools, and allowing them to cease and desist the work of any information system or website that was used to commit crimes included in the law. This means that the prosecutor of the State Security Court, which is not recognised internationally, will have the authority to enter and search without being held accountable."*[17]

15. In order to be lawful and in respect with international human rights law, communications surveillance must meet the minimum standards of being enshrined in clear and public laws, being necessary in a democratic society to achieve a legitimate aim and proportionate to that aim. Individuals must be protected against arbitrary interference with their right to communicate privately. When a government wishes to conduct communications surveillance, it must only be done in accordance with clear and transparent law.[18]

16. It is therefore urgent that Jordan address the legal and regulatory void which law enforcement and security agencies in Jordan are currently operating in. Jordan must legislate to regulate surveillance activities conducted by law enforcement and security agencies as soon as possible.

Obligations on Internet Cafe and Monitoring of Users

17. In 2010, the "Instructions/Guidance for regulating the work of internet cafes and centres" was amended to require that the cafe owner check the identity of all users and to keep their browsing history for six months. The cafes are routinely visited by a committee of representatives from General Intelligence Department, Public Security Directorate, Communications Ministry and other officials. This committee has the right to check these records and make recommendations to the specialized governor.

18. The most recent amendment to Article 6 of "Instructions/Guidance for regulating the work of Internet cafes and centres, and the basis of their licensing and amendments (2016)"[19] requires internet cafe owners "to take all procedures and arrangements" to make sure that their users are not engaging in terrorism-related or any illegal activities while browsing the internet. This new provision

[16] Available in Arabic at: http://www.lob.jo/View_LawContent.aspx?ID=865

[17] Almasri, R., Cybercrime Law – How does the government control the online platform?, 7iber, 30 January 2018, available at: https://www.7iber.com/technology/cyber-crime-law-how-does-the-government-control-the-online-platform/

[18] See: International Principles on the Application of Human Rights to Communications Surveillance, available at: https://necessaryandproportionate.org/principles; Privacy International, Explainer: Communications Surveillance, available at: https://privacyinternational.org/explainer/1309/communications-surveillance

[19] Available in Arabic at: http://www.ammanchamber.org.jo/Uplaoded/PRNews/802.pdf

would require internet cafe owners to monitor the activities of who use their facilities. However, the provision does not specify the exact "procedures and arrangements" that the cafe owner must follow, and neither nor the exact activities they should prevent users from pursuing. This leaves a lot of room for this provision to be misinterpreted and abused.

Mandatory SIM Card Registration

19. There is a mandatory SIM card registration policy in Jordan. Anyone wanting to purchase a SIM card will have to provide their national ID card, or a passport in case of foreigners, to activate a new prepaid SIM card.[20] The regulation creating the system also states that at any moment, the Ministry of Interior can request additional documentation be provided during the registration process.

20. The Telecommunication Regulatory Commission announced in January 2018 that it will develop new regulations that will require new owners of SIM cards to submit their fingerprints to authenticate their lines.[21] It is still not clear how the measure will be implemented or what legal basis that does the Commission have to develop the said regulation.[22]

21. SIM registration undermines the ability of users to communicate anonymously and disproportionately disadvantages certain groups of society which for different reasons may not have a national ID card. It also facilities surveillance and makes tracking and monitoring of users easier for law enforcement authorities.

Surveillance Capabilities

22. Whilst the extent of Jordan's surveillance apparatus is known over the years there has been reported evidence indicating that Jordan has attempted to expand its surveillance capabilities. A leak of emails from the Italian surveillance malware vendor Hacking Team in July 2015 has shown that the Jordanian government has been interested in developing its surveillance capabilities. Emails dating back to mid-2011 show direct, regular correspondence between Jordanian officials in the General Intelligence Department and Hacking Team's keymanagers.[23] Beside the General Intelligence Department, other intended beneficiaries of Hacking Team's services were Jordan's police[24] and the army.[25]

[20] Instructions for regulating the work of points of sale of mobile lines and their amendments, 2015, available at: http://www.qistas.com/legislations/jor/view/3694202. Other regulations added security requirements for shops in 2017. See: http://www.ammanchamber.org.jo/Uplaoded/3453.pdf

[21] Available in Arabic at: http://trc.gov.jo/DetailsPage/TRC_AR/TenderAr.aspx?ID=127

[22] See: Royal News, 10 January 2018, available in Arabic at: http://royanews.tv/news/145755

[23] See relevant documentation on Jordan published by Wikileaks on 5 July 2015, including: https://wikileaks.org/hackingteam/emails/emailid/616353, https://wikileaks.org/hackingteam/emails/emailid/12039m, and https://wikileaks.org/hackingteam/emails/emailid/575695.

[24] Available at: https://wikileaks.org/hackingteam/emails/emailid/1135003

[25] Available at: https://wikileaks.org/hackingteam/emails/emailid/601419

23. It has been also documented how some telecommunications companies are using Deep Packet Inspection equipment, consisting in data solutions installed between the customers and the Internet that have the ability to filter, block and intercept Internet communications.[26]

II. DATA PROTECTION

24. Jordan currently does not have a comprehensive data protection law. This lack of adequate and comprehensive legislation on data protection is of particular concern given that the increasing creation of data intensive systems in Jordan, such as SIM card registration issues, smart identification cards, among other systems.

25. In 2014, the Ministry of Communications submitted a draft bill for the protection of personal data, and a public consultation was announced in November 2016. A committee was formed for the purpose of discussing the law that included the Ministry of the Interior, Ministry of Labour and Ministry of Communications, in addition to the Telecommunications Regulatory Commission, the Central Bank and Information and Communications Association of Jordan (INTAJ). Civil society groups including 7iber, JOSA, INTAJ, Taqaddam, and other organisations, have studied the draft bill and provided recommendations based on internationally recognised data protection principles and standards.

26. In 2017, the ICT Ministry published a new draft of the bill, which raisesmajor concerns, notably the absence of an independent data protection authority with financial and administrative independence, the lack of consideration for modern forms of personal data processing, and its lack of incorporation of international standards and best practices.

27. Identification cards have been issued since 1955 and in 2016, the Department of Civil Status (Ministry of Interior) and the Ministry of Information and Telecommunication Technology introduced a new smart national ID card. In addition to the information of the old card, the new cards will include a chip (144 KB) to store biometric data like an iris scan and fingerprints. The smart identity card includes 18 data fields, such as gender, the name in Arabic and English, place of birth, area of residence, and blood type, and in later stages, the card expects to include information about such issues as health insurance, pension, and voting activities.[27]

28. No specific regulations have been adopted[28] to regulate the deployment of the smart ID card, and the lack of a data protection law, as mentioned before, leaves this kind of initiative without clear regulation for the processing and

[26] See: Qurium, Internet Blocking in Jordan, available at: https://www.qurium.org/alerts/jordan/internet-blocking-in-jordan/

[27] See: Gemalto, Jordan Launches its new ID card pogram, 1 March 2018, available at: https://www.gemalto.com/govt/customer-cases/national-id-card-jordan

[28] The most related piece of legislation seems to be the Civil Status Law, available in Arabic at: http://www.qistas.com/legislations/jor/view/3652250

security of personal data.[29] Most decisions on the issue have been adopted directly by the Prime Minister and their cabinet,[30] with limited oversight and involvement from other stakeholders.[31]

29. At the end of 2017, the Department of Personal Status (Ministry of Interior) announced March 2018 as the final date for citizens to exchange their old national ID with the new one.[32] After that date no official or private entities will acknowledge any other forms of identification. This cut-off data raises concerns as having a card is mandatory to enrol in the electoral register, and also there are plans for the new ID card to integrate driving license information and health insurance data.[33]

30. In 2009, Jordan began implementing the Hakeem national e-health health records programme.[34] This programme, implemented by the Jordanian non-profit organisation Electronic Health Solutions, creates a database of patients' medical histories,[35] including the diseases they suffer from and all tests and procedures they have undergone. The system links patients to their national ID number and is also designed to help future research and statistical analysis.[36]

31. In 2015, the Greater Amman Municipality signed a 3-year institutional agreement with Microsoft Jordan "to provide modernity and advanced technology" and to turn Amman into a "smart city".[37] Even though the reported agreement is over, other similar initiatives have been announced,[38] all looking forward to create data intensive systems in the city government, despite the lack of proper legislation to address personal data protection in the country.

32. There have also been reports about increasing presence of CCTV and Speed cameras in Amman.[39] The number of reported installed cameras in Amman is of 720, however it is not clear whether they have been used for traffic monitoring or for surveillance purposes.[40] The lack of privacy laws regulating the operation

29 See: The Hashemite Kingdom of Jordan, The Official Site of the Jordanian e-Government, available at: https://jordan.gov.jo/wps/portal/Home/SmartCard

30 Available in Arabic at: https://bit.ly/2I4SL48

31 Available in Arabic at: https://bit.ly/2pLVb11 and https://bit.ly/2pLVb11

32 See: AlGhad, 13 September 2017, available in Arabic at: http://www.alghad.com/articles/1826862-بادصإ-2-5-قيلاذ-ةقاطب-نوبلم

33 See: Zawya, Gov't to offer 350 e-services by end of 2019 – minister, 15 August 2016, available at: https://www.zawya.com/mena/en/story/Govt_to_offer_350_eservices_by_end_of_2019__minister-ZAWYA20160816052400/

34 Further information available at: http://ehs-int.com/about-hakeem

35 The Jordan Times, E-health programme to be implemented nationwide, 16 November 2015, available at: http://www.jordantimes.com/news/local/e-health-programme-be-implemented-nationwide

36 Open Health News, EHS and the Hakeem Program Continue to Successfully Implement 'Open' EHR Systems in Jordan, 11 June 2013, available at: http://www.openhealthnews.com/hotnews/ehs-and-hakeem-program-continue-successfully-implement-open-ehr-systems-jordan

37 Optomiza, Optimiza and GAM Sign an Agreement to Transform Amman into a Smart City, 19 March 2015, available at: http://optimiza.me/agreement-amman-smart-city/

38 Anaxza Med, Jordan to build new smart city worth billions, 7 November 2017, available at: http://www.ansamed.info/ansamed/en/news/sections/economics/2017/11/07/jordan-to-build-new-smart-city-worth-billions_0c296a0e-f910-4820-9bee-77479440b019.html

39 AlGhad, GAM to Increase Traffic Cams in Amman; 33 New Installations Soon, 22 September 2017, available at: http://english.alghad.com/articles/1844222-GAM-to-Increase-Traffic-Cams-in-Amman-33-New-Installations-Soon

40 More information see: The Arab Weekly, Jordan receives advanced anti-terror training from United States, 21 March 2018, available at: https://thearabweekly.com/jordan-receives-advanced-anti-terror-training-united-states

of these cameras raise several questions regarding the existence of any restrictions on the use of CCTV footage for surveillance, or other issues.

33. With the increasing initiatives requiring the processing of personal data of Jordanians, it is urgent for Jordan to adopt and enforce a comprehensive data protection law to ensure the protection of personal data of it citizens through an open, inclusive and transparent legislative process.

RECOMMENDATIONS

34. We recommend that the government of the Jordan:

- Initiate process to legislate on communication surveillance by all state entities, including law enforcement and security agencies, to ensure that all communications activities are conducted in respect for the right to privacy and comply with Jordan's national and international human rights obligations;
- Reform anti-terrorism law and other related legislation to add substantive and procedural safeguards in order to clarify and review oversight mechanisms over the surveillance practices of its state security and intelligence agencies, to ensure compliance with the right to privacy, and integrate monitoring and audit of these;
- Establish independent accountability mechanisms and clear standards for Jordan's security and intelligence agencies to ensure they are subject to independent oversight mechanisms and guarantee the transparency of their mandate and operations in accordance with international human rights standards;
- Review all licensing agreements which impose obligations on the private sector to facilitate and/or conduct communication surveillance, and take the necessary measures to ensure that the private sector – in both policy and practice – comply with international human rights law and standards, in particular in relations to requirements for blanket, indiscriminate data retention;
- Disclose what type of surveillance technologies are employed by Jordanian law enforcement and intelligence agencies, how their acquisition and use is regulated and monitored and how are they complying with the law and the Constitution;
- Conduct prompt and independent investigations into credible reports of unlawful surveillance of lawyers, journalists, human rights activists and others, with the view to bring to justice the perpetrators and provide reparations. Publish the results of these investigations;
- Adopt and enforce a comprehensive data protection law to ensure the protection of personal data of it citizens through an open, inclusive and transparent legislative process, and creating an independent oversight body with sufficient funding and enforcement powers.