Privacy International's Comments on the draft Prevention of Electronic Crimes Act, 2015 (Pakistan)

April 2015

Privacy International reiterates the serious concerns expressed together with Digital Rights Foundation Pakistan about the proposed Prevention of Electronic Crimes Bill in Pakistan. The Bill introduces a series of new provisions that pose a grave risk to freedom of expression and privacy in Pakistan.

In the context of growing concerns over government surveillance of activists, bloggers, journalists, as well as ordinary internet users and the expanding surveillance capacity of Pakistani authorities, particularly intelligence agencies, the Bill, if adopted in the current form, will further undermine the protection of the right to privacy, freedom of expression and other human rights. As it stands the Bill is also contrary to Pakistan's obligations under international law, notably the International Covenant on Civil and Political Rights to which Pakistan is party.

Beyond the general concerns expressed in the joint statement, Privacy International raise the following concerns related to specific provisions of the Bill. The comments are based in our experience promoting the right to privacy internationally across multiple legal frameworks.

1. Information-sharing with foreign governments and entities should be regulated by specific laws and subject to independent oversight
2. A clear and accessible legal regime compliant with international law should govern any data copied by state authorities
3. Requiring mandatory retention of traffic data by service providers threatens the right to privacy

4. Service providers should not be required to keep investigation or the fact of real-time collection and recording of data secret indefinitely
5. Unauthorised issuance of SIM cards should not lead to mandatory SIM card registration and be detrimental to anonymity
6. Power to obtain decryption of information needs to be strongly regulated

1. Information-sharing with foreign governments and entities should be regulated by specific laws and subject to independent oversight

Draft section 37 would allow for cooperation between the Federal Government and foreign governments, foreign agencies and others in terms of the Act. Specifically, draft subsection (2) would permit the Federal Government to forward information obtained from investigations under the Act to foreign agencies or international agencies. A prior request from the foreign entity would not be required to exercise this power.

This broad power to share information with foreign entities is troubling. The information at stake is expansive: "text, message, data, voice, sound, database, video, signals, software, computer programs, codes including object code and source code".[1] The information shared could include particular sensitive information about individuals or large quantities of data involving significant numbers of people. Once this information has left the hands of the Federal Government, it would no longer be subject to national law and could be used by foreign entities as they see fit. This poses significant risks to the right to privacy.

Information-sharing with foreign entities should be regulated by a specific law which establishes strong oversight mechanisms and provides for domestic accountability mechanisms. Data should only be transferred to foreign jurisdictions where there are strong legal and procedural safeguards in place to ensure the right to privacy is respected.

2. A clear and accessible legal regime compliant with international law should govern any data copied by state authorities

In the draft law the definition of "seize", with respect to program or data, includes "making and retaining a copy of the data"(Section 2, Definitions,

1 Under the definition proposed by the Act (as defined in clause (o) of the Electronic Transactions Ordinance, 2002).

z.) However, the draft law does not specify the procedures through which seized data is retained, stored, deleted or further copied. It also does not regulate the sharing of data among government entities. Instead, in draft Section 33 it merely says that the Federal Government may prescribe rules for dealing with the information system, data or other articles seized.

These elements should be specifically enumerated and governed by a clear and accessible legal regime that provides for redress for any violations of the right to privacy. Data should not be retained for longer than is necessary, given the purposes for which it was collected. Nor should it be used for purposes outside those specified in the draft law. If an existing law already operates in this area, it should be referenced within the draft law.

3. Requiring mandatory retention of traffic data by service providers threatens the right to privacy

Draft section 29 would require a service provider, a term that the proposed bill defines broadly, to "within its existing or required technical capability, retain its traffic data minimum for a period of one year or such period as the Authority may notify from time to time". Traffic data is defined to include "data relating to a communication indicating its origin, destination, route, time, size, duration or type of service" (draft section 2, definitions, (cc).)

We note that this requirement may already be in place under the Electronic Transaction Ordinance, 2002 and suggest that it should be discontinued.

Imposing a requirement on service providers to retain traffic data runs contrary to protecting the right to privacy. Even more so, as such retention would be for a minimum of one year, significantly longer than 90 days envisaged in an earlier draft, and service provider could be required to retain potentially indefinitely, at the discretion of the Authority set up by this law. Such a provision helps to create the conditions under which invasive surveillance of populations is able to take place.

The interception, collection and use of metadata interfere with the right to privacy as has been recognized by human rights experts including the UN Special Rapporteur on freedom of expression, the UN Special Rapporteur on counter-terrorism and human rights and the High Commissioner for Human Rights.[2] The Court of Justice of the European Union noted that

2 See report of the UN Special rapporteur on the promotion and protection of the freedom of opinion and expression, UN doc. A/HRC/23/40, 17 April 2014; report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, UN doc. A/69/397, 23 September 2014, and report of the UN High Commissioner for Human Rights, Right to Privacy in

metadata may allow "very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained" and concluded that the retention of metadata relating to a person's private life and communications is, in itself, an interference with the right to privacy.[3]

4. Service providers should not be required to keep investigation or the fact of real-time collection and recording of data secret indefinitely

Draft section 35 (subsection 3) requires that "the service provider, for a period not exceeding fourteen days, shall keep confidential and not disclose the existence of any investigation or exercise of any power under this Act when a notice to this effect is served upon it by an authorised officer, which period of confidentiality may be extended beyond fourteen days if, on an application by the authorised officer, the Court authorises an extension for a further specified period, upon being satisfied that reasonable cause for such extension exists."

We have significant concerns about this provision: first, the requirement of confidentiality for the first 14 days does not require court's authorisation, and is at the sole discretion of the authorised officer. Secondly, there is no maximum time limit to the extension of such confidentiality that a court may grant.

More broadly, the exercise of powers under the Act must be open to scrutiny; at a minimum, an independent oversight mechanism should have the ability the examine any orders made under this section and publish the fact of their existence.

Draft section 36 would permit real-time collection and recording of data in specified circumstances. We reiterate the importance of ensuring that any such collection and recording is undertaken in accordance with international human rights standards protecting the right to privacy.[4]

We note with concern that draft subsection (3) allows the Court to extend the period of such real time collection and recording beyond 7 days without setting any maximum time limit.

---

the Digital Age, UN doc. A/HRC/27/37, 30 June 2014.

3 See Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, Judgment of 8 April 2014.

4 See the International Principles on the Application of Human Rights to Communications Surveillance: https://en.necessaryandproportionate.org/text

We also note with concern draft subsection (4), that "[t]he Court may also require the designated agency to keep confidential the fact of the execution of any power provided for in this section and any information relating to it".

5. Unauthorised issuance of SIM cards should not lead to mandatory SIM card registration and be detrimental to anonymity

Draft Section 15 criminalises the selling or providing of SIM card or other memory chips designed for transmitting or receiving information without obtaining and verifying the subscriber antecedents in the manner approved by the Authority. Punishment for such a crime would be imprisonment for up to 3 years and/or a fine.

Mandatory SIM registration is already in effect in Pakistan. We are concerned that the introduction of this crime will eradicate the ability of mobile phone users to communicate anonymously and facilitates mass surveillance, making tracking and monitoring of all users easier for law enforcement and security agencies. The potential for misuse of such information is enormous. SIM registration can also have discriminatory effects – the poorest individuals (many of whom already find themselves disadvantaged by or excluded from the spread of mobile technology) are often unable to buy or register SIM cards because they do not have identification documents or proof of residence. The justifications commonly given for SIM registration – that it will assist in reducing the abuse of telecommunications services for the purpose of criminal and fraudulent activity – are unfounded. SIM registration has not been effective in curbing crime, and instead has fueled the growth of identity-related crime and black markets to service those wishing to remain anonymous.[5]

6. Power to obtain decryption of information needs to be strongly regulated

Under draft Section 32 (subparagraph g) an authorised officer has the power to "require any person who is in possession of decryption information of an information system, device or data under investigation to grant him access to such decryption information necessary to decrypt data required for the purpose of investigating any such offence."

---

5 See Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN doc. A/HRC/23/40, 17 April 2013.

While the provision provides certain guidance on the way such power should be exercised (acting with proportionality, avoiding disruption, seizing data only as a last resort), the powers vested on the officer are very broad and particularly invasive of the privacy of individual's digital communications. Their potential for misuse is extremely high. This is particularly so as the power provided could be used to demand the disclosure of encryption keys, thereby exposing individuals at the risk of disclosure of private data beyond what may be necessary to conduct an investigation.