PRIVACY INTERNATIONAL

DigitalRightsFoundation
"KNOW YOUR RIGHTS"

ARTICLE 19

The Prevention of Electronic Crimes Bill 2015 - An Analysis

June 2016

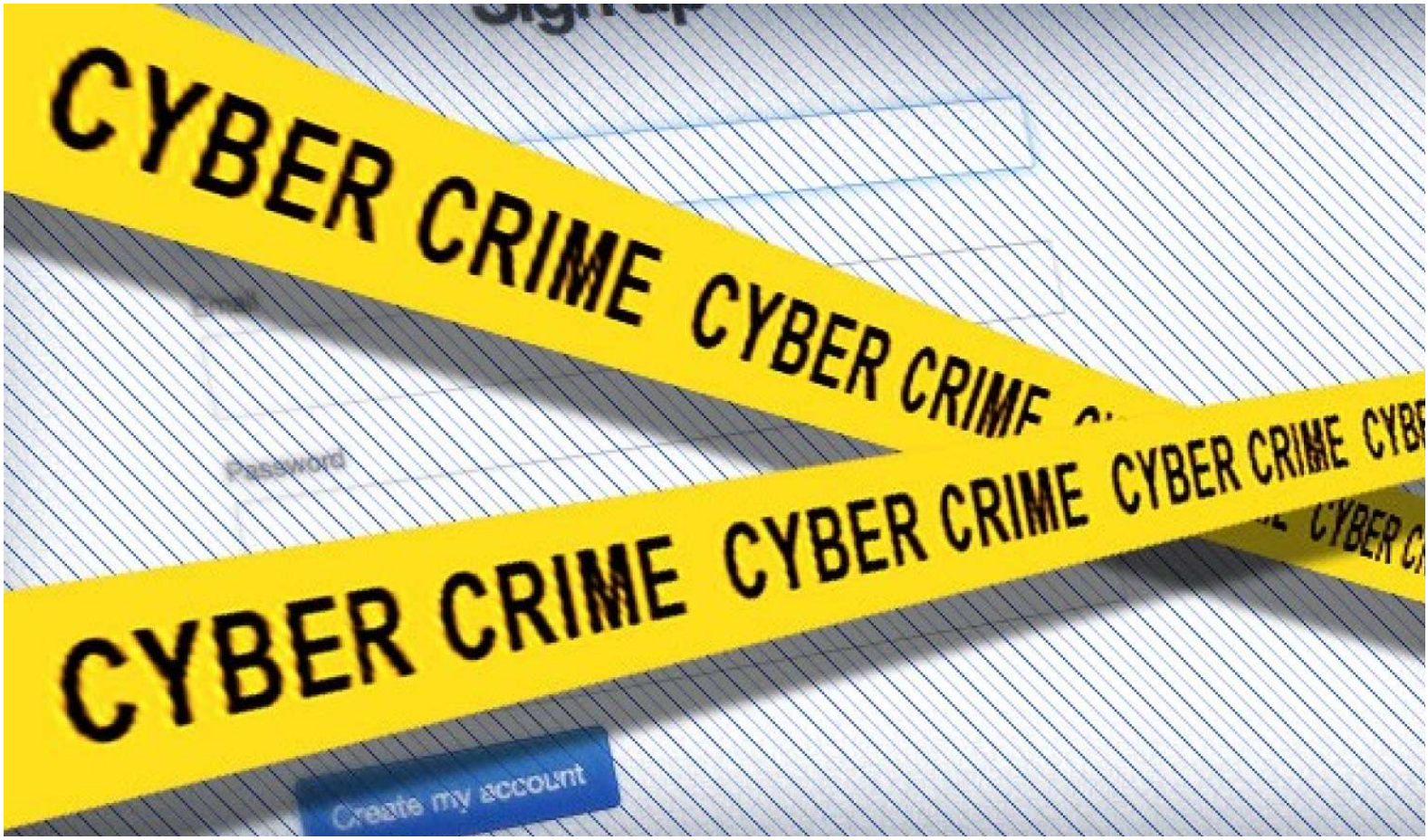

Table of Contents

Table of Contents 2
Prevention of Electronic Crimes Bill - A Context 4
PECB - A Timeline 6
January 2015 6
February 2015 6
April 2015 6
May 2015 6
August 2015 7
September 2015 7
October 2015 7
December 2015 7
January 2016 8
February 2016 8
April 2016 8
May 2016 8
PECB Falls below International Standards on Freedom of Expression 10
Our Concerns 10
1. Overly broad definitions (clause 2): 10
Recommendations 12
2. Glorification of an offence and hate speech (clause 9): 12
Recommendations: 12
3. Overbroad offences against misuse of computers and lack of public interest defence (clauses 3 to 8): 13
Recommendations: 14
4. Overly broad cyber-terrorism offence (clause 10): 14
Recommendation: 15
5. Offences against dignity of natural persons (clause 18): 15
Recommendation: 16
6. Offences against the modesty of a natural person and minor (clause 19): 16
Recommendations: 17

7. Cyberstalking (clause 21): 17
Recommendation: 18
8. Unlawful online content (clause 34): 18
Recommendation: 18
9. Overly broad preventive measures (clause 45): 18
Recommendation: 19
10. Spoofing (clause 23): 19
Recommendation: 19
11. Criminalising the production, distribution and use of encryption tools (clauses 13 to 16): 19
Recommendation: 20
12. Miscellaneous: 20
Recommendations: 20
PECB's privacy and surveillance problems 21
Unauthorised issuance of SIM cards should not lead to mandatory SIM card registration and be detrimental to anonymity 22
Requiring mandatory mass retention of traffic data by service providers violates the right to privacy 23
Broad powers of the authorized officers, including power to request decryption of information, needs to be subjected to independent, judicial oversight 24
Service providers should not be required to keep investigation or the fact of real-time collection and recording of data secret indefinitely 25
Information-sharing with foreign governments and entities should be regulated by specific laws and subject to independent oversight 26

Prevention of Electronic Crimes Bill - A Context

On April 13, 2016 the National Assembly's Standing Committee on Information Technology and Telecommunication approved the Prevention of Electronic Crimes Bill (PECB).The failure to release the document publicly until May 7, two days before the convening of the Senate of Pakistan, reinforces the lack of transparency and open consultation that has marked the government's approach concerning the legislative process behind the PECB. Throughout the process, the NA Standing Committee on IT has chosen to consult behind closed doors, keeping civil society organisations outside and avoiding public oversight. The PECB has been heavily criticised by several Pakistani and international organisations, as well as the United Nations' Special Rapporteur on freedom of opinion and expression[1].

The NA Standing Committee has also sought to prevent its own members from examining drafts of the PECB. When the PECB was first approved by the National Assembly Standing Committee on IT in September 2015 it was revealed that the approved draft had been shared with the chairman of the standing committee, but not the rest of the committee[2]. Legitimate objections – that the Bill could not be approved until the draft had been read by the rest of the committee – were overruled by the standing committee chairman, on the grounds that as he had seen it, and that was sufficient for approval. PPP MNAs Shazia Marri and Nauman Islam Sheikh, had rightly stressed that the draft PECB could not be approved until they and the other members of the committee had read the finalised draft. This bypassing of necessary review by the committee as a group was criticised by Senator Sherry Rehman via twitter[3].

There has been a complete lack of transparency by the government of the drafting process of a piece of legislation that will have serious consequences for the rights of privacy and freedom of expression of Pakistani citizens. The situation has drawn the attention and concern of the UN Special Rapporteur on the promotion of the right to freedom of expression, David Kaye. The Special Rapporteur released a statement in December 2015, urging the government to ensure that the PECB respect freedom of expression, or else "if adopted, the draft legislation could result in censorship of, and self-censorship by, the media" and other segments of society.

Civil society and other stakeholders have consistently called upon the government to implement amendments that respect and protect the rights to privacy and freedom of expression of Pakistani citizens. Until now, these calls have been largely ignored. What we ask is that the Senate not only dismiss the Bill, but that the PECB be redrafted to address the problematic provisions previously identified. Whilst, a cybercrime bill is necessary in the world we live in, the PECB has been flawed from its inception, claiming the importance of security over civil liberties, and must be rebuilt from the ground up, with careful and considered input from all civil society stakeholders. In its current

---

1 "UN expert urges Pakistan to ensure protection of freedom of expression in draft Cybercrime Bill", Statement of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression David Kaye, United Nations Office of The High Commissioner for Human Rights, December 14, 2015 http://bit.ly/1TRCaz2

2 "Draft cybercrime bill bulldozed through NA body", Dawn, September 18, 2015 http://www.dawn.com/news/1207737

3 "Opposition Comments on PECB", Bolo Bhi, Accessed May 16, 2016, http://bolobhi.org/opposition-on-pecb/

form, the Bill and the possibility for it to become law, remains a danger to, rather than a protector of, the rights of Pakistani citizens. The Senate must take the opportunity to not only return the Bill back to the Committee, but it must also ask that the Bill be redrafted entirely, and to take on the comments and input of the Senate and of civil society.

PECB - A Timeline

The timeline below indicates the trajectory and series of events that mark the flawed nature of the consultative process from the inception of the 2015 PECB, to the current state of affairs:

January 2015

The Prevention of Electronic Crimes Bill 2015, a revamping and reintroduction of the Prevention of Electronic Crimes Act 2014, is announced, in the context of the National Action Plan, and in the wake of the attack on the Army Public School in December 2014. It is reported by The News that the Ministry of IT will be forwarding the PECB for tabling in the National Assembly after drafting it "in consultation with other stakeholders". Said consultations, however – made both before and after the bill was drafted – were largely ignored by the government.[4]

February 2015

Pakistani and international rights organisations – Digital Rights Foundation, Privacy International, Article 19 – issue legal analyses examining the provisions within the Bill, and the concerns of civil stakeholders, pertaining in particular to:

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 should govern any data copied and retained by state authorities

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

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

April 2015

April 13, the National Assembly IT Standing Committee passes the fourth version of the PECB. Revisions and amendments are made that in effect criminalise freedom of expression, interfere with the right to privacy, and curtail civil liberties. This again occurs behind closed doors, without any input or consultation of civil society stakeholders. Joint statements and advocacy initiatives by local and international civil society organisations, Bolo Bhi, Bytes for All, Digital Rights Foundation, Human Rights Watch, Pakistan for All, Article 19, and Privacy International – eventually lead to a tentative opening up of the drafting process.

May 2015

The chairman of the NA Standing Committee on IT puts out a call to the public for comments, seeking concerns regarding the PECB and its flaws. However, the public consultation is opened only for seven days. The chairman of the NA Standing Committee, furthermore, insists stakeholders were

4 "A Fading Opportunity to Protect Internet Freedom in Pakistan", Freedom House, March 13, 2015, https://freedomhouse.org/blog/fading-opportunity-protect-internet-freedom-pakistan

consulted over the past three years. The Joint Action Committee – made up of civil society stakeholders – submits aggregated comments accordingly.

A public hearing on the PECB is scheduled, but only seven people – not organisations – were invited" to speak before the committee. The JAC and other civil society organisations call for actual public hearings on the PECB.

Minister for IT, Ms. Anusha Rehman, falsely and grossly misrepresents the concerns of stakeholders, saying that "elements are making a hue and cry so that no laws against cybercrimes could be enacted in the country."[5] Civil society organisations and other stakeholders have consistently emphasised that while a cybercrime bill is required, the PECB is detrimental to the rights of Pakistani citizens, and is not right for citizens, the media or the IT industry, have also been strongly critical of the PECB.

August 2015

A meeting is called to approve the Bill, to which members of the committee raise serious reservations, in particular that there is no prior notice given, save for one day before the session. PPP MNA Shazia Marri files a letter of dissent in regards to the PECB, along with suggested amendments. http://bolobhi.org/wp-content/uploads/2015/11/Dissent_Shazia-Marri.pdf

September 2015

The NA Standing Committee on IT approves the draft of the PECB. It is later revealed that copies of the draft were not shared with other members, and the chairman declared that as he had seen the draft, and approved of it, this was sufficient. This was done despite the objections of PPP MNAs Shazia Marri and Nauman Islam Sheikh, and PML-N MNA Awais Ahmad Khan Leghari, who rightly stressed that the draft bill could not be approved until they and the other members of the committee had read the finalised draft. This bypassing of necessary review by the committee is critiqued by Senator Sherry Rehman via twitter.

October 2015

Senator Sherry Rehman reiterates (via an interview with Express Tribune) that a "toothcomb review" of the bill is vital to "eliminate and amend provisions which are in grave violations of Article 19 of the UN Charter, of which Pakistan is a signatory."[6]

December 2015

The UN Special Rapporteur on freedom of opinion and expression, Mr. David Kaye, releases a statement urging that the PECB ensure "protection of freedom of expression". The concern is that , "if adopted, the draft legislation could result in censorship of, and self-censorship by, the media."

---

5 "Citizens and Industry Refute IT Minister's Statements & Demand Proper Public" Bolo Bhi, Accessed May 20, 2015, http://bolobhi.org/citizens-and-industry-refute-it-ministers-statements-demand-proper-public-hearing/

6 "PPP vows to block cybercrimes bill" Express Tribune, October 7, 2015 http://tribune.com.pk/story/968594/in-senate-ppp-vows-to-block-cybercrimes-bill/

January 2016

Chairman of the Senate Standing Committee on IT, Mr. Shahi Syed (ANP) expresses his concern regarding the PECB: "There was no need to bring such a controversial bill which is against freedom of speech."[7]

February 2016

The February 2016 draft of the PECB is released. This is the version, plus amendments by Ms. Anusha Rehman[8], that is passed by the NA in April 2016. The same concerns remain as this draft of the PECB continues to threaten the rights of freedom of expression and privacy of Pakistani citizens.

April 2016

The PECB is passed by the NA on April 13– however, this occurs with over 90% of Members of the National Assembly absent.

In an April 14 interview with 92 News, Mr. Aitzaz Ahsan, Leader of the Opposition in the Senate, and a member of the PPP says that the PPP rejects the PECB, and will not pass it in the Senate.[9]

May 2016

Despite becoming a public document upon being passed by the NA, it takes almost 3 weeks – early May – for the PECB to be uploaded to the NA website and for it to become publicly available. It currently awaits scrutiny from the Senate.

---

7 "PECB 2016: Will not pass the bill in Senate, says Syed", Express Tribune, January 9, 2016 http://tribune.com.pk/story/1024303/pecb-2016-will-not-pass-the-bill-in-senate-says-syed/

8 "The Prevention of Electronic Crimes Bill 2015 Conundrum – Major Documents " Digital Rights Foundation, Accessed May 16, 2016 http://digitalrightsfoundation.pk/the-prevention-of-electronic-crimes-bill-2015-conundrum-major-documents/

9 "PPP rejects Cyber Crime Bill – Aitzaz Ahsan" Television Interview, April 14, 2016 http://www.dailymotion.com/video/x44h5d7

DigitalRightsFoundation

"KNOW YOUR RIGHTS"

ANALYSIS BY ARTICLE 19 & DIGITAL RIGHTS FOUNDATION

PECB Falls below International Standards on Freedom of Expression

ARTICLE 19 and Digital Rights Foundation have serious concerns about the latest draft of the Prevention of Electronic Crimes Bill ('PEC Bill'), that was passed by the National Assembly on 13 April 2016.[10] While the PEC Bill contains some limited improvements, particularly in relation to the new cyberstalking offence, we are disappointed that the vast majority of our comments on a previous version of the Bill have been ignored.[11] In this statement, we therefore largely reiterate the concerns we had raised previously. In our view, the Bill contains a number of provisions that, if implemented, would violate the rights to freedom of expression and privacy. We urge members of the Senate of Pakistan to carefully consider our comments to ensure that any new cybercrime legislation is fully compliant with international human rights standards.

Our Concerns

In ARTICLE 19 and Digital Rights Foundation Pakistan's view, the PEC Bill violates international standards on freedom of expression for the following reasons:

1. **Overly broad definitions (clause 2):** at the outset, we note that several definitions contained in clause 2 of the Bill are unduly broad, in particular:

   "act" is defined in clause 2 (a) (i) as a "series of acts or omissions contrary to the provisions of this Act". In our view, this definition is both unclear and unnecessary. First, 'act' is defined by reference to a 'series of act' without ever defining what an 'act' means. Furthermore, 'act' is defined as including omissions, i.e. a failure to act, which is potentially confusing.

   "access to data" is defined in clause 2 (b) as "gaining control or ability to read, use, copy, modify, or delete any data held or generated by any device or information system" (our emphasis). In our view, however, "gaining control" over data, including "reading, using, copying, modifying or deleting" it, go far beyond mere access. This broad definition is likely to create a significant overlap between the various offences against computer misuse under clauses 3 to 8.

   "access to information systems" in clause 2 (c) is similarly broadly defined as 'gaining control or ability to use any part or whole of an information system'. However, mere "access" does not necessarily imply such control or ability to use an information system.

[10] http://www.na.gov.pk/uploads/documents/1462252100_756.pdf
[11] https://www.article19.org/data/files/medialibrary/37932/Pakistan-Cybercrime-Joint-Analysis_20-April-2015.pdf

"*critical infrastructure"* is defined in clause 2 (j) as infrastructure, which is "vital" to the State Pakistan or other Pakistani institutions and "such that its incapacitation disrupts or adversely affects national security, the economy, public order, supplies, services, health, safety or matters incidental or related thereto". ARTICLE 19 and Digital Rights Foundation believe that this definition sets too low a threshold for what constitutes "critical infrastructure". In particular, clause 2 (j) provides that the incapacitation of such infrastructure would merely "disrupt" or "adversely affect" the interests listed in the definition. In our view, however, "critical infrastructure" means that the *destruction* or *incapacitation* of such infrastructure would have a *debilitating* effect on national security, the economy, public health and safety or other *essential* national or public services, rather than "matters merely incidental or related thereto". In other words, critical infrastructure must mean infrastructure, without which the State could not function.

"data damage" is defined in clause 2 (n) as "alteration, deletion, deterioration, erasure, relocation, suppression of data or making data temporarily or permanently unavailable". However, the mere "alteration, deletion, erasure, suppression or relocation or data" does not necessarily entail damage to that data. Damage can only occur by reference to *impairment* to the normal functioning of an information system (or something).

"*dishonest intention"* is defined in clause 2 (p) as including intention "to cause injury" or "to create hatred". In our view, however, intention "to cause injury" is not dishonest as such but malicious. Similarly, "intention to cause hatred" is not intrinsically dishonest. Moreover, it is both vague and potentially confusing.

"interference with information system or data" is defined in clause 2 (v) as including "an unauthorised act in relation to an information system or data that may disturb its normal working or form with or without causing any actual damage to such system or data". In our view, this definition is unnecessary and likely to overlap with the offence of interference with information system or data under clause 5. Moreover, we believe that the definition in clause 2 (v) fails to properly define what amounts to an interference, e.g. by reference to the alteration, deletion, deterioration, damage or suppression of data. It also sets too low a threshold for such an interference to take place. In our view, rather than merely potentially "disturbing" the normal functioning of information systems or data "without causing any actual damage", an interference should at least "seriously hinder" the functioning of information systems. We further note that the Council of Europe Cybercrime Convention 2001, which represents a benchmark in the area of cybercrime, does not define "interference with information systems or data" but rather lays down two separate offences, namely "data interference" (Article 4) and "system interference" (Article 5).

"*unauthorised access"* is defined in clause 2 (zf) as "access to an information system or data which is not available for access by the general public, without authorisation or in violation of the terms and conditions of the authorisation". We doubt that this is definition is necessary. In particular, we note that the Council of Europe Cybercrime Convention 2001

does not seek to define "unauthorised access". Moreover, the definition appears to be largely tautological.

Recommendations

- Clause 2 (j) should be more narrowly defined. "Disrupt or adversely affect" should be struck off and replaced by "debilitate", "essential" should be inserted before "supplies", "and public" should be inserted before "services" and "or matters incidental or related thereto"" should be removed.
- Clause 2 (p) should distinguish dishonest from malicious intent.
- The other definitions outlined above are unnecessary and should be removed.

2. **Glorification of an offence and hate speech (clause 9):** the April 2016 version of the PEC Bill retains the offence of "glorification of an offence and hate speech" under clause 9 with some minor amendments compared to earlier versions. In particular, it now specifies the type of offences (crimes related to terrorism) and activities (those of proscribed organisations) whose glorification is criminalised. Despite these changes, we remain of the view that this offence is drafted in overly broad terms in breach of international standards on freedom of expression. In particular, the criminalisation of the 'glorification of an offence or the person accused or convicted of a crime relating to terrorism or activities of proscribed organisations' under clause 9 would stifle debate on matters of public interest, including national security, as well as the application of the criminal law in individual cases. Furthermore, the previous UN Special rapporteur on Freedom of Expression, Frank La Rue, made it clear in his May 2011 report that the term 'glorification' fails to meet the requirement of legality under international human rights law. The same is equally true of terms such as "support" of terrorism, which are wholly unclear.

Recommendations*:*

- Clause 9 should be removed in its entirety.
- To the extent that the Pakistani government may wish to prohibit incitement to discrimination, hostility or violence or incitement to terrorism, it should do so consistently with the requirements of international standards on freedom of expression. In this regard, we note that the four special mandates have held in their 2008 Joint Declaration on defamation of religions, and anti-terrorism, and anti-extremism legislation that:

  "The criminalisation of speech relating to terrorism should be restricted to instances of intentional incitement to terrorism, understood as a direct call to engage in terrorism which is directly responsible for increasing the likelihood of a terrorist act occurring, or to actual participation in terrorist acts (for example by directing them). Vague notions such as providing communications support to terrorism or extremism, the 'glorification' or 'promotion' of terrorism or extremism, and the mere repetition of statements by terrorists, which does not itself constitute incitement, should not be criminalised."

3. **Overbroad offences against misuse of computers and lack of public interest defence (clauses 3 to 8):** in our analysis of earlier drafts of the Bill, we had noted that offences against misuse of computers or 'hacking' types offences failed to provide for a public interest defences for cases where unauthorised access to information systems, programmes or data may take place for legitimate purposes, such as investigative journalism or research.[12] These concerns remain unaddressed. In our view, this is a missed opportunity for the Prevention of Cybercrime Bill to promote a progressive, forward-looking approach to the protection of freedom of expression in cybercrime legislation.

   The April 2016 version of the Bill introduces six offences against misuse of computers (clauses 3 to 8), three of which are specifically targeted at attacks on critical infrastructure information systems or data (clauses 6 to 8). Despite the welcome introduction of a higher threshold regarding *mens rea* (dishonest intent), these provisions could be more narrowly drafted and would benefit from additional safeguards. For instance, clause 3 of the Bill criminalises "whoever with dishonest intention gains unauthorised access to any information system or data". The offence is punishable by imprisonment for a term, which may extend to 3 months or a fine of up to 50,000 rupees or both. Contrary to best practice under the Cybercrime Convention, however, there is no requirement that security measures must be infringed in order for the *actus reus* of the offence to be completed. Moreover, the definitions of "access to data" and "access to information systems in clauses 2 (b) and (c) respectively are so broad that the offence contained in clause 3 significantly overlaps with the offences contained in clauses 4 and 5.

   Similar concerns apply to clause 5 of the Bill, which introduces the offence of interference with information system or data without requiring that such interference result in *serious* harm. Reference is only made to "interference" or "damage". In the absence of a serious harm requirement or a public interest defence, the Bill fails to recognise that interest groups may legitimately engage in peaceful 'online protest' by seeking to disrupt access to a website without causing any real damage to that site. This would be the case, for instance, if traffic to a government webpage were temporarily redirected to an interstitial webpage containing a lawful message. **In our view, this is not remedied by the requirement of dishonest intent given its broad definition under clause 2 (p)**

   Even more disturbingly, clause 4 of the Bill criminalises the unauthorised copying or transmission of "any" data "without authorisation". Whilst the offence includes a requirement of 'dishonest intent', there is absolutely no requirement for such data to be unlawful in any way for the prohibition on copying or transmission to apply. Furthermore, clause 4 does not include any protection for journalists or whistleblowers, who may copy or transmit information without authorisation in the public interest. We also note that the Cybercrime Convention does not include any requirement for States to adopt any provisions of this kind. In our view, this provision is much too broad and in breach of the legality requirement under international human rights law.

[12] https://inforrm.wordpress.com/2012/05/16/investigative-journalism-and-the-criminal-law-the-dpps-guidelines-and-the-need-for-a-public-interest-defence-alex-bailin-qc-and-edward-craven/

The above concerns equally apply to the equivalent offences introduced in relation to critical infrastructure information system or data (clauses 6 to 8). These concerns are especially acute given the overbroad definition of critical infrastructure in clause 2 (j).

Recommendations*:*

- Clauses 3-5 should be revised and at a minimum be brought more closely in line with the requirements of the Cybercrime Convention.
- A public interest defence should be introduced for 'hacking'-type of offences.

4. **Overly broad cyber-terrorism offence (clause 10):** the cyber-terrorism offence remains drafted in excessively broad language. The concerns we highlighted in our March 2014 and April 2015 statements remain unaddressed. Cyber-terrorism offences must be much more clearly linked to violence and the risk of harm and injury in the real world and in particular harm against the welfare of individuals. In particular, any coercion or intimidation must be directed at individuals and create a sense of fear or panic in the public or section of the public rather than the Government as currently provided in clause 10 (a). At the very least, cyber-terrorism offences should be much more clearly linked to severe disruptions or destruction of critical infrastructure and their impact in the real world. In this sense, it is highly unclear how the mere unauthorised access to critical infrastructure information systems or data, or the unauthorised copying or transmission of critical infrastructure data, or threat to do the same, necessarily has the effect of causing serious harm or injury to individuals in the real world.

   Contrary to clause 10 (b), we further note that terrorism offences should not be confused with offences prohibiting the advocacy of hatred, which constitutes incitement to violence, hostility or discrimination.

   While there is no internationally agreed definition of cyber-terrorism, we draw attention to the model definition of terrorism proposed by the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism has proposed the following model definition of terrorism:

   "Terrorism means an action or attempted action where:

   1. *The action:*
      (a) Constituted the intentional taking of hostages; or
      (b) Is intended to cause death or serious bodily injury to one or more members of the general population or segments of it; or
      (c) Involved lethal or serious physical violence against one or more members of the general population or segments of it;

      AND

2. *The action is done or attempted with the intention of:*
   (a) Provoking a state of terror in the general public or segment of it; or
   (b) Compelling a Government of international organisation to do or abstain from doing something

   AND

3. *The action corresponds to:*
   (a) The definition of a serious offence in national law, enacted for the purpose of complying with international conventions and protocols relating to terrorism or with resolutions of the Security Council relating to terrorism; or
   (b) All elements of a serious crime defined by national law." (A/HRC/51, para. 28). "

Recommendation:

- Clause 10 should be revised in light of the above concerns and brought more closely in line with the model definition of terrorism outline above.

5. **Offences against dignity of natural persons (clause 18):** Clause 18 (1) of the Bill punishes with criminal sanctions "whoever intentionally and publicly exhibits or displays or transmits any information, through any information system, which he knows to be false, and intimidates or harms the reputation or privacy of a natural person". We note that efforts have been made to narrow the scope of this provision, including by introducing a knowledge requirement in relation to false information and a more affirmative requirement that such information should cause 'harm' or 'intimidate' the reputation or privacy of natural persons. Nonetheless, we stand by our earlier comments that this provision effectively criminalises defamation in breach of international standards on freedom of expression. In its General Comment no. 34 the UN Human Rights Committee stated that States parties should consider the decriminalisation of defamation and that criminal law should only be applied in the most *serious* cases. Moreover, even where defamation is a civil wrong, the law should provide that a statement is not defamatory unless its publication has *caused* or is likely to cause *serious* harm to the reputation of the claimant.

   We further note that the language of clause 18 is problematic in that privacy is generally breached by the disclosure of information, which is true rather than false. Moreover, leaving aside that privacy and reputation cannot be intimidated as such, 'intimidation' is a separate concept from the harm that may arise from the dissemination or disclosure of false or true information. In other words, clause 18 is unclear as it seeks to cover too many different privacy wrongs under one (overbroad) heading of 'offences against the dignity of natural persons'.

   More generally, we take the view that the publication of private information in breach of confidence or the misuse of private information should be treated as civil wrongs rather than criminal offences as is the case under the PEC Bill. We are further concerned that clause 18 (2) provides for a new remedy that would allow aggrieved persons to apply for injunctions ordering the removal, destruction or blocking of access to material in breach of clause 18 (1).

Although attempts at protecting the right to privacy and reputation are legitimate, we believe that these types of injunctions are ineffective at achieving their stated purpose due to the nature of the Internet itself. In particular, in the case of blocking measures, there is a real risk that access to legitimate information may be restricted due to well-known attendant risks of overblocking or underblocking.

Recommendation*:*

- Clause 18 should be removed.

6. **Offences against the modesty of a natural person and minor (clause 19):** clause 19 of the PEC Bill introduces a new offence against the modesty of a natural person or minor. In particular, clause 19 (1) criminalises "whoever intentionally and publicly exhibits, displays or transmits any information which (a) superimposes a photograph of the face of a natural person over any sexually explicit image; or (b) distorts the face of a natural person or the inclusion of a photograph or a video of a natural person in a sexually explicit conduct; or (c) intimidates a natural person with any sexual act; or (d) cultivates, entices, induces a natural person to engage in a sexually explicit act. The above acts are criminalised when committed with intent to "harm a natural person or his reputation, or to take revenge, or to create hatred or to blackmail".

   Again, while attempts to protect the dignity of natural persons are laudable, and with the exception of clause 19 (c), we question whether the criminal law is the most effective way of dealing with these types of behaviour. In particular, we note that new clause 19 (d) is unclear, excessively broad and unnecessary. For instance, it is highly unclear what sort of information might entice or 'cultivate' someone to engage in a sexually explicit act.

   While we note efforts to narrow the scope of clause 19 (1) by introducing a requirement of intent to 'harm a natural person or his reputation, or to take revenge, or to create hatred or to blackmail', a requirement of intent to cause mere 'harm' – rather than '*serious* harm' – or 'to create hatred' is overly broad. Furthermore, and in any event, allowance should be made for the fact that sexually explicit images may be used for journalistic purposes, e.g. to report on the character of politicians or public officials. Equally, superimposing someone's image over a sexually explicit image may be used as a form of humour, e.g. in caricatures to distil a political message (see, *mutatis mutandis*, Palomo Sanchez v Spain, ECtHR, 12 September 2011). Although the introduction of the new intent requirement goes some way towards alleviating these concerns, a more affirmative defence for the protection of freedom of expression would be strongly desirable. This is especially so given that, as currently drafted, the requirement of intent 'to create hatred' could be used against journalists and others who publish videos mocking particular politicians.

   Clause 19 (3) effectively criminalises the production and dissemination of child pornography. In our view, this is a very serious matter that warrants a standalone provision rather than

being lumped together with broad offences against the modesty of a natural person or a minor.

Clause 19 (4) provides for a new remedy that would allow aggrieved persons to apply to the (Pakistan Telecommunication) Authority for injunctions ordering the removal, destruction or blocking of access to information in breach of Clauses (1) and (3). Clause 19 (4) further provides that the Authority may direct any of its licensees to secure such information including traffic data. We note that international law permits website blocking for the purposes combatting child pornography provided that the national law is sufficiently precise and there are effective safeguards against abuse or misuse, including oversight and review by an independent and impartial tribunal or regulatory body (see A/HRC/17/27 at para. 32). However, we are deeply concerned that the Authority does not provide such independent oversight (see also our concerns regarding clause 34 further below). Moreover, we reiterate our concern that blocking is ineffective due to the very real risk that access to legitimate information may be restricted due to well-known attendant risks of overblocking or underblocking. This is a matter of special concern in circumstances where clause 19 (1) is overly broad and therefore likely to criminalise information, which should be considered legitimate. Furthermore, we note that clause 19 (4) potentially empowers the Authority to order ISPs to use technology, such as deep packet inspection, to monitor online content in breach of international standards on freedom of expression and privacy. In this regard, the four special mandates on freedom of expression have held in their 2011 Joint Declaration on Freedom of Expression that "content filtering systems which are imposed by a government or commercial service provider and which are not end-user controlled are a form of prior censorship and are not justifiable as a restriction on freedom of expression".

Recommendations*:*

- With the exception of clause 19 (3), clause 19 (1)-(2) and (4) should be removed or at least revised in light of the above concerns.
- Clause 19 (3) should become a standalone provision on child pornography.

7. **Cyberstalking (clause 21):** ARTICLE 19 and Digital Rights Foundation note that clause 21, which criminalises cyberstalking, has been significantly improved compared to earlier drafts. We nonetheless question the need for specific offences in this area. In our view, it would be better to deal with the underlying mischief in such cases by way of general provisions against harassment, stalking, intimidation and threats of harm under the Criminal Code. Notwithstanding this more general concern, we believe that clause 21 (3), which provides for blocking injunctions, is unnecessary. Leaving aside the problems raised by blocking injunctions, which we've already expressed above, we consider that website blocking is unlikely to be the most effective way of dealing with stalkers. Rather, it appears that court injunctions ordering defendants to stop harassing or stalking victims, including by preventing communication between them, would be more appropriate (see e.g. protection orders under South Africa Protection from Harassment Act 2011). Finally, we note that clause 21 (1) (d) could be further improved by specifying the type of harm caused by the

taking of a photograph or making of a video of a person without his or her consent (e.g. severe distress, anxiety etc.).

Recommendation:

- Clause 21 (3) should be removed and replaced with court injunctions protecting victims from harassment or stalking.

8. **Unlawful online content (clause 34):** we remain concerned that clause 34 of the Bill grants new sweeping powers to the Pakistan Telecommunications Authority ('PTA') to order the removal or blocking of access to "any" information if it considers it necessary 'in the interests of the glory of Islam' or the 'integrity, security or defence of Pakistan' or on the grounds of 'public order, decency or morality, or in relation to contempt of court or commission of or incitement to an offence. In other words, this section grants *carte blanche* to the government to restrict access to any information on the Internet it dislikes without a determination of the legality of the content at issue by a court. The grounds on which access to such information may be restricted go far beyond the legitimate aims exhaustively listed under Article 19 of the International Covenant on Civil and Political Rights. This includes for instance the 'glory of Islam', and 'decency'. Moreover, and any event, the clause entirely fails to provide for a right of appeal or judicial review of the decisions of the PTA. Instead, clause 34 (2) merely provides that the Authority may "with the approval of the Federal Government" prescribe rules for adoption of standards and procedure for the exercise of powers under clause 34 (1). In short, clause 34 is overly broad and fails to include adequate safeguards for the protection of the rights to freedom of expression and privacy in breach of international human rights law.

Recommendation*:*

- Clause 34 should be rejected in its entirety.

9. **Overly broad preventive measures (clause 45):** ARTICLE 19 and Digital Rights Foundation are further concerned that clause 45 provides the Federal Government or the Authority with far-reaching powers to issue any guidelines to information systems service providers as long as it is "in the interests of preventing any offence under this Act". Under clause 45 (2), violations of the guidelines by information systems service providers are criminalised. In our view, this provision is clearly in breach of the legality requirement under Article 19 (3) ICCPR as it grants the government powers to issue any guidelines that it likes, however unreasonable or restrictive of freedom of expression. Moreover, it criminalises the violation of guidelines, which remain undefined and may well be arbitrary. In other words, information systems services providers could be held criminally liable for failing to implement guidelines, which cannot be implemented on a practical level. This clause is therefore entirely arbitrary and in breach of well-established criminal law principles that

individuals and companies should be able to foresee the circumstances in which they may find themselves criminally liable.

Recommendation*:*

- Clause 45 should be rejected in its entirety.

10. **Spoofing (clause 23):** Clause 23 introduces a new offence of spoofing. While this section is presumably aimed at dealing with counterfeiting websites, we are concerned that it fails to provide sufficient safeguards against its potential misuse against individuals setting up humorous websites mocking well-known brands. While the requirement of 'dishonest intent' goes some way towards alleviating this problem, we believe that clause 23 should provide for a clearer defence for the protection of freedom of expression. In the absence of such defence, we believe that the offence in its current form is overly broad and risks having a serious chilling effect on the right to freedom of expression. We also note that spoofing seemingly criminalises a different type of conduct in other countries, such as the United States where it is used in criminal proceedings involving a form of market manipulation.

Recommendation*:*

- Clause 23 should be further narrowed in line with our recommendations above.

11. **Criminalising the production, distribution and use of encryption tools (clauses 13 to 16):** we are concerned that clauses 13 and 16 may be used to criminalise the production, distribution and use of encryption tools enabling anonymity online. Clause 13 criminalises whoever produces, makes, generates, adapts, exports, supplies, offers to supply or imports for use any information system, data or device intending *or believing it primarily to be used* to commit or to assist in the commission of an offence under this Act. In our view, this provision could be used to crack down on software programmers who produce goods that may be used for both legitimate and illegitimate purposes. In particular, programmes such as Tor enable users to be anonymous online. The Bill makes no distinction between a tiny proportion of users who might use anonymity for criminal purposes and the vast majority of legitimate users of such anonymity tools who simply wish to protect their right to privacy whilst reading or sharing information online. Given the borderless nature of the Internet and the differences between the types of cyber-offences from country to country, it would be impossible to establish whether a programmer knew, intended or 'primarily believed' the programme to be used for the commission of an offence. In any event, it would constitute a disproportionate restriction on the exercise of freedom of expression and the right to privacy.

    Clause 16 further criminalises whoever unlawfully or without authorisation changes, alters, tampers with or re-programmes unique device identifiers of any communication equipment and starts using or marketing such device for transmitting and receiving information. We are concerned that this provision might be used to crackdown on manufacturers, suppliers and

users of programmes such as Tor or proxy servers that enable anonymous browsing online. In our view, this is a disproportionate restriction on the exercise of the right to freedom of expression as well as the right to read and browse anonymously online.

Recommendation*:*

- Both clauses 13 and 16 should be removed. At the very least, "or believing" and "primarily" in clause 13 should be struck off.

12. **Miscellaneous:** ARTICLE 19 and Digital Rights Foundation are concerned that clauses 48 (power to make rules) and clause 49 (removal of difficulties) give broad powers to the Government to legislate in this area by way of regulations or statutory instruments that would enable it to further restrict the rights to freedom of expression and privacy. In our view, this is undesirable and should be avoided.

    Finally, we note that clause 24 provides for the legal recognition of offences committed in relation to information systems. We query the need for such a provision. As we've noted elsewhere in these comments, we believe that, as a general rule, offences should be technology neutral. Therefore, aside from online behaviours that have clearly been recognised under international law as requiring a specific response, e.g. under the Cybercrime Convention, we believe that the general criminal law should be used to tackle issues, which arise both online and offline such as harassment or incitement to discrimination, hostility or violence. Furthermore, we question whether the inclusion of information system and data into the definition of 'property' "in any law creating an offence in relation to property" is appropriate in the absence of an analysis as to whether such crimes are relevant to information systems or data and whether this might not lead to the duplication of offences that would risk creating further legal uncertainty.

    Moreover, the offence of electronic forgery is unclear, in particular, the intent requirement "with the intent to cause damage or injury to the public or any person" is much too broad, it is also unclear that the 'intent to commit fraud by any input etc." is necessary given that the next offence is supposed to deal with fraud.

Recommendations:

- At the very least the Senate should consider restricting the number of areas in which the Government retains powers to legislate by way of statutory instruments and regulations, particularly as regards clause 48 (2) (b), (c) and (h).
- Clause 49 should be removed.
- Clause 24 should be removed.

PRIVACY INTERNATIONAL

DigitalRightsFoundation
"KNOW YOUR RIGHTS"

ANALYSIS BY PRIVACY INTERNATIONAL & DIGITAL RIGHTS FOUNDATION

PECB's privacy and surveillance problems

We reiterate the serious concerns expressed about the proposed Prevention of Electronic Crimes Bill in Pakistan. We note that the Bill adopted by the National Assembly in April 2016 includes some improvements compared to the earlier version, including by introducing some safeguards on the storage of information and data acquired by authorized officers. However, as currently drafted 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 contrary to Pakistan's obligations under international law, notably the International Covenant on Civil and Political Rights to which Pakistan is party.

We raise the following concerns related to specific provisions impacting on the right to privacy. The comments are based on applicable international human rights standards and on our experience promoting human rights internationally across multiple legal frameworks.

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.[13]

Recommendation:

[13] 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.

- Draft Section 15 should be removed.

Requiring mandatory mass retention of traffic data by service providers violates 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 for a minimum period of one year or such period as the Authority may notify from time to time and provide that data to the investigation agency or the authorized officer whenever so required."

Traffic data is defined broadly to include "data relating to a communication indicating its origin, destination, route, time, size, duration or type of service".[14]

We note that this requirement may already be in place under the Electronic Transaction Ordinance, 2002 and recommends 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 traffic data 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.[15] The Court of Justice of the European Union noted that traffic data 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.[16]

---

[14] Section 2, Definitions, (zd).

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

[16] 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.

Alternatives to mass data retention exist, including targeted preservation orders. Under this model, the government would request the preservation of communications data of specific individuals based on an investigation or proceeding.[17]

Recommendation:

- Remove the requirement of data retention contained in draft Section 29.

Broad powers of the authorized officers, including power to request decryption of information, needs to be subjected to independent, judicial oversight

Section 32 lists the powers of the authorised officers to conduct searches and seizure of data.

These powers are very broad, particularly given that he or she would also have the power to "require any person having charge of or otherwise concerned with the operation of any information system to provide him reasonable technical and other assistance as the authorized officer may require for investigation of an offence" (draft Section 32, subparagraph f.)

While Section 32, subsection (2) provides certain guidance on the way such power should be exercised (acting with proportionality, avoiding disruption, seizing data only as a last resort), there is nothing in the Bill that stipulate how the exercise of these powers are subjected to independent, judicial oversight. As such the potential for misuse of these powers is extremely high.

This is particularly so as the power provided could be used to demand the disclosure of encrypted information, thereby exposing individuals at the risk of disclosure of private data beyond what may be necessary to conduct an investigation. 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 data, device or information system in unencrypted or decrypted intelligible format for the purpose of investigating any such offence."

As noted by the UN Special Rapporteur on the freedom of expression, "key disclosure or decryption orders often force corporations to cooperate with Governments, creating serious challenges that implicate individual users online. […] In both cases, however, such orders should be based on publicly accessible law, clearly limited in scope focused on a specific target, implemented

[17] The United States government, for example, relies on data preservation, rather than data retention. Pursuant to the Stored Communications Act, the government may make a "preservation request" to service providers to "take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process." 18 U.S.C. §2703(f). The period of retention is 90 days, which can be extended for another 90 days upon a renewed government request.

under independent and impartial judicial authority, in particular to preserve the due process rights of targets, and only adopted when necessary and when less intrusive means of investigation are not available. Such measures may only be justified if used in targeting a specific user or users, subject to judicial oversight."[18]

Recommendation:

- Review draft Section 32, in particular subparagraphs f and g to limit the overbroad powers of officers to conduct search and seizure of data.

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) provides that "Provided 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 authorized officer, which period of confidentiality may be extended beyond fourteen days if, on an application by the authorized officer, the Court authorizes an extension for a further specified period upon being satisfied that reasonable cause for such extension exists."

We welcome the provision that requires Court's authorization for any extension of the period of confidentiality. However, we are concerned that 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 Bill 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 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, nor requiring that the Court applies a strict test of necessity and proportionality to assess whether such extension is warranted.

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".

Recommendations:

[18] See Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN doc. A/HRC/29/32, 22 May 2015, paragraph 45.

- Set a maximum time limit in draft Section 35(3) and ensure that the court review any request for confidentiality and examine whether confidentiality is strictly necessary for the purposes of the investigation;
- Review draft Section 36(4) to require the court to examine whether confidentiality is strictly necessary for the purposes of the investigation.

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

Section 39 of the Bill 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.

This broad power to share information with foreign entities is troubling. It covers "any information obtained from its own investigations" with "information" defined broadly to include "text, message, data, voice, sound, database, video, signals, software, computer programmes, any forms of intelligence as defined under the Pakistan Telecommunication (Re-organization) Act, 1996 (XVII of 1996) and codes including object code and source code".[19]

The information shared could include particular sensitive information about individuals or large quantities of data involving significant numbers of people.

To share such information will all be at the sole discretion of the Pakistani government: no requirement of judicial authorization, either from the requesting foreign government or Pakistan; nor in fact any prior request from the foreign entity would not be required to exercise this power.

Once this information has been transferred, it could be used by foreign entities as they see fit. The wording of sub-section 3 provides no guidance of the kind of conditions or limitations that the Pakistani government may seek to impose to the use of such information, nor on the mechanisms to ensure such conditions are adhered to.

This poses significant risks to the right to privacy. As noted by UN human rights experts, including the UN Special Rapporteur on counter-terrorism and human rights and the Human Rights Committee, lack of adequate regulation of intelligence sharing have resulted in the sharing of individual's communications with foreign agencies without appropriate safeguards.[20] The Human Rights Committee has specifically recommended that a robust oversight system over intelligence-

[19] Section 2, Definitions, (s).
[20] See report of the UN Special Rapporteur on counter-terrorism and human rights, UN doc. A/69/397, 23 September 2014.

sharing is in place, "including by providing for judicial involvement in the authorization of such measures in all cases"[21]

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.

Recommendation:

- Remove draft Section 39.

[21] See Concluding observations on the United Kingdom, UN Doc. CCPR/C/GBR/CO/7, 17 August 2015.