



CENTRE FOR LAW
AND DEMOCRACY

Pakistan

Comments on the Prevention of Electronic Crimes Act, 2014

March 2014

Centre for Law and Democracy
info@law-democracy.org
+1 902 431-3688
www.law-democracy.org

Introduction¹

The spread of the Internet, while providing unprecedented benefits in terms of development and freedom of expression, also poses novel challenges from a regulatory perspective. Legal frameworks governing issues such as communication, commerce and privacy need to be adapted to align with the changes wrought by the digital transition. To this end, the government of Pakistan commissioned a team of lawyers, led by Akram Shaikh and Aslam Hayat, to develop new cybercrime legislation. The resulting draft law, which was submitted to the Ministry of Information Technology in early 2014, has now been developed into the draft Prevention of Electronic Crimes Act, 2014 (the draft Act). According to our sources, now that it has been approved by the Ministry, the draft Act will be submitted to Cabinet for approval before being presented to Parliament.

There is, without question, a pressing need for governments around the world to draft legislation which enables full advantage to be taken of the digital transition. While some legal frameworks can be easily applied in an online context, others require substantial adaptation. It is, in this context, critically important to ensure that any legislation which impacts on freedom of expression is consistent with recognised international human rights standards. This is particularly important since a significant part of the Internet's value as an expressive medium flows from its open and borderless nature, qualities which can only be preserved through a light regulatory touch. In order to harness fully the power of the Internet, with all of the economic, cultural and expressive benefits that it entails, the people of Pakistan must be allowed to communicate freely online.

The draft Act has many positive features, including robust procedural and evidential rules governing the work of investigators and clear protection for online intermediaries. However, several of the newly created cybercrimes are overly broad and threaten to criminalise innocuous, commonplace or even beneficial online behaviour. The draft Act also proposes a data retention scheme, the implementation of which could severely undermine privacy and freedom of expression in Pakistan.

These Comments examine the major issues with the draft Act from a freedom of expression perspective, and provide concrete recommendations for how the law should be amended to bring it into line with international human rights standards. Although we welcome the Pakistani government's decision to consider legislation on

¹ This work is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported Licence. You are free to copy, distribute and display this work and to make derivative works, provided you give credit to Centre for Law and Democracy, do not use this work for commercial purposes and distribute any works derived from this publication under a licence identical to this one. To view a copy of this licence, visit: <http://creativecommons.org/licenses/by-nc-sa/3.0/>.

this important issue, it is critically important that the law which is finally adopted is carefully calibrated to safeguard the vibrancy of the online discourse.

1. Background

The vast majority of cybercrimes are digital variations of crimes that have existed for decades. For example, while computer fraud and cyber stalking may seem like new phenomena, in many jurisdictions these types of behaviours are already covered by existing laws against fraud and criminal harassment. As a result, while it is important to update official understandings of how crimes are committed in a digital environment, the need to create new cybercrimes can be overstated.

Some criminal activities are, however, specific to a digital context, such as the generation and intentional spread of computer viruses, and may, therefore, necessitate new legislation. Given the increasing centrality of the Internet to freedom of expression, it is critically important that new legislation regulating online behaviour respect the following three-part test for restrictions on this right enumerated in Article 19(3) of the *International Covenant on Civil and Political Rights* (ICCPR),² which Pakistan ratified in June 2010:

The exercise of the rights provided for in paragraph 2 of this article [freedom of expression] carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

- (a) For respect of the rights or reputations of others;
- (b) For the protection of national security or of public order (ordre public), or of public health or morals.

According to Article 19(3), restrictions on the right to freedom of expression are only legitimate if they are consistent with this test. This means that restrictions must be clearly spelled out in law, must aim to protect one of the legitimate interests listed in Article 19(3), and must be necessary for the protection of that interest. The latter means, among other things, that any restrictions must be designed so as to impair freedom of expression as minimally as possible. The UN Human Rights Committee has summarised these conditions as follows:

Restrictions must not be overbroad. The Committee observed in general comment No. 27 that "restrictive measures must conform to the principle of proportionality; they must be appropriate to achieve their protective function; they must be the least intrusive instrument amongst those which might achieve their protective function; they must be proportionate to the interest to be protected...The principle of proportionality has to be respected not only in the law that frames the restrictions but also by the administrative and judicial authorities in applying the law". The principle

² UN General Assembly Resolution 2200A(XXI) of 16 December 1966, in force 23 March 1976.

of proportionality must also take account of the form of expression at issue as well as the means of its dissemination. For instance, the value placed by the Covenant upon uninhibited expression is particularly high in the circumstances of public debate in a democratic society concerning figures in the public and political domain.

When a State party invokes a legitimate ground for restriction of freedom of expression, it must demonstrate in specific and individualized fashion the precise nature of the threat, and the necessity and proportionality of the specific action taken, in particular by establishing a direct and immediate connection between the expression and the threat. [references omitted]³

The importance of defining offences as narrowly as possible is of heightened importance due to the relatively low rate of Internet penetration in Pakistan. According to the International Telecommunications Union, as of 2012 only 9.6% of Pakistanis used the Internet.⁴ This can be compared to an Internet penetration rate of 43.2% in China and 84.1% in South Korea. Given that many Pakistanis are still discovering the Internet, it is crucial to avoid criminalising normal online behaviours. The potential for a chilling effect, whereby individuals steer well clear of the potential zone of application to avoid censure, is magnified significantly in this case due to the relative novelty of the medium.

2. Unauthorised Access and Usage

Several of the new offences defined in the draft Act are problematic primarily because they are overbroad. Section 3 makes it a crime to access an information system without authorisation or in excess of authorisation, while section 4 makes it a crime to access a programme or data without authorisation or in excess of authorisation. According to section 3(1), the prohibition includes “instances where there may exist general authority to access an information system but a specific type, nature or method of access may not be authorised.” The maximum penalty for breaching section 3 is six months imprisonment and/or a fine of one hundred thousand rupees (approximately USD950), while section 4 carries a maximum penalty of nine months imprisonment and/or a fine of two hundred thousand rupees (approximately USD1,900). Both section 3 and section 4 may also be engaged in a context of mere recklessness, albeit with mitigated penalties compared to the intentional commission of these offences. Although both sections require that the crimes be committed knowingly, section 2(2) defines that term as including not just actual awareness, but also circumstances where a person specifically avoids taking steps to confirm his or her belief that a particular state of affairs exists or will exist.

³ General Comment No. 34, 12 September 2011, CCPR/C/GC/34, paras. 34 and 35.

⁴ Statistics available at: <http://www.itu.int/net4/itu-d/icteye/>.

While the aim of these provisions is presumably to combat hacking, their wording criminalises enormous amounts of innocuous behaviour. Nearly every information system, including many websites, contains a terms of use agreement dictating the precise way in which the product or service is authorised to be used. These documents frequently contain binding conditions. For example, the website for Hilton Hotels contains an agreement which states that users must be at least eighteen years of age.⁵ The *New York Times* website's terms of service mandates that all users must be "courteous" and "respectful".⁶ Other common stipulations are that users must live within or outside particular jurisdictions, or that they will not be offended by the content contained therein. End-user licence agreements are also routinely included with hardware devices, such as computers or smartphones, as well as most software purchases. In each case, the agreement contains strict conditions governing how the information system may legitimately be used.

Given the length of these agreements and the frequency with which digital consumers are presented with them, they are nearly universally ignored. This is generally not a problem since the main function of these agreements is to provide protection for the service provider against liability of one form or another. It is highly unlikely that the *New York Times* will ever seek a legal remedy against users who fail to observe proper courtesies. However, by making it a criminal offence to use an information system or access data without authorisation, or in excess of the authorisation received, the draft Act essentially turns any breach of these terms of service into a criminal offence. The fact that knowledge of a lack of authorisation can be inferred if a user fails to take adequate steps to inform themselves of the conditions of access means that breach of these terms of use can attract criminal liability regardless of whether or not users have read them. Users who wish to stay on the right side of the law would have to slog through pages of terms and conditions for every website they visit and any device or programme they use, to ensure that they are not using the service beyond the dictates of its creator.

There are also legitimate motivations for why users might seek to operate a system in excess of authorisation. For example, many electronic artistic works are protected by a digital rights management (DRM) system. These are designed to stop illegal copying, but they can also prevent legitimate uses which engage copyright's exceptions (such as the creation of transformative derivative works). In most cases where a DRM system has been imposed, there is no practical legal avenue to remove it, even for a legitimate reuse. Users who seek to circumvent DRM systems in pursuit of activities which are legitimate under copyright law should not face criminal sanction.

⁵ Available at http://www.hilton.com/en/hi/info/site_usage.jhtml.

⁶ Available at: <http://www.nytimes.com/content/help/rights/terms/terms-of-service.html#discussions>.

In order to ensure that innocuous conduct is not targeted for prosecution, sections 3 and 4 should be limited to instances where the breach was committed with the intention of obtaining an illegitimate commercial or other advantage or of causing commercial loss or some other harm, such as an invasion of privacy or undermining security. The government should also consider removing the “recklessness” standard from these as well as other provisions in the draft Act. Considering Pakistan’s relatively low levels of Internet penetration, many users will be on a learning curve in relation to digital technologies. Although section 2(2)(c) clarifies that the “reckless” standard will be applied according to a subjective standard (evaluating each individual according to their level of experience and understanding), this rule is still likely to exert an unfortunate chilling effect on Internet use. Furthermore, it is difficult to conceive of circumstances where an unintentional breach of the rules would ever justify a criminal prosecution.

Sections 5 and 6, which prohibit any unauthorised alteration of a programme or data, or interference with an information system, are similarly problematic, since they also criminalise the circumvention of DRM measures taken in pursuit of legitimate reuses. In addition, it is important to recognise the benefits that come from allowing digital consumers to customise or tinker with products, just as a purchaser of an automobile might want to install a new transmission or engine. Alteration of data or a programme or interference with an information system should only be subject to criminal sanction where the act was undertaken with the intention of obtaining an illegitimate commercial or other advantage or of causing commercial loss or other harm, such as the targeting of government infrastructure in a manner that is not in the public interest.

Recommendations:

- Sections 3 to 6 should be limited to instances where the breach was undertaken with the intention of obtaining an illegitimate commercial or other advantage or of causing commercial loss or other harm.
- The draft Act’s recklessness standards should be removed.

3. Privacy

Respect for privacy is key to preserving freedom of expression on the Internet. It is broadly recognised that privacy, and the ability to communicate free from surveillance, are necessary to democratic discourse. As the UN Special Rapporteur on Freedom of Opinion and Expression noted:

The Centre for Law and Democracy is a non-profit human rights organisation working internationally to provide legal expertise on foundational rights for democracy

States cannot ensure that individuals are able to freely seek and receive information or express themselves without respecting, protecting and promoting their right to privacy.... Without adequate legislation and legal standards to ensure the privacy, security and anonymity of communications, journalists, human rights defenders and whistleblowers, for example, cannot be assured that their communications will not be subject to States' scrutiny.⁷

Anonymity is of paramount importance in an online context due to the pervasive nature of surveillance online. Both State actors and private companies spend billions of dollars attempting to track every move that users make. In response to these intrusions, the use of pseudonyms has become extremely common on the Internet, as are software programmes which alter a user's online signature in an attempt to hide his or her identity.

In this context, section 8(1) of the draft Act, which deals with electronic forgery, is problematic inasmuch as it makes it a crime to input "inauthentic data". The presentation of inauthentic data is key to the functionality of most privacy software. While these tools can be used in the commission of crimes, the vast majority of their users simply do not like being watched and seek nothing more nefarious than basic online privacy. In order to foster the development of the Internet in Pakistan, it is critically important to allow users avenues to enhance online privacy. Sections 8(2) and 8(3) – which bar electronic forgery for various purposes, such as to create wrongful financial gains or losses or to influence public servants or public information systems – are sufficient safeguards against actual fraud.

Those who create anonymity tools could also potentially face liability under section 10, which prohibits the creation or transfer of devices which are intended for use in criminal offences under the draft Act or which are known to be likely used for the commission of offences. As noted above, savvy cyber criminals are likely to employ privacy software in order to maximise their chances of evading detection. However, the fundamental purpose of this software is benevolent, in that it is designed to help protect privacy not to facilitate the commission of criminal activities. As a result, its creators and hosts should not face prosecution. It should be noted that section 26 imposes limitations on intermediary liability by requiring malicious intent and positive participation, which would seem to immunise most service providers. However, the potential for conflict between sections 10 and 26 would best be resolved by amending the former so that it only applies to devices which are designed primarily for the commission of offences.

Recommendations:

⁷ Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 17 April 2013, UN Doc. A/HRC/23/40, para. 79.

- Section 8(1), which makes it a crime to input inauthentic data, should be removed.
- Section 10 should only apply to devices that are designed primarily for the commission of offences.

4. Cyber-terrorism and Other Offences

Section 7 provides that anyone who commits or threatens to commit offences under sections 5 or 6 for the purpose of terrorism faces more severe penalties, up to fourteen years imprisonment and/or a fine of fifty million rupees (approximately USD 475,000). While stiffer penalties are justified in dealing with actions that severely damage public institutions, it is difficult to justify such long prison terms simply for threats to commit crimes. It is also inappropriate to levy terrorism charges against anyone who “enables” the crime, as is done in section 7(1)(b)(vii). This term is not defined. While it is appropriate to prosecute individuals who wilfully aid or abet crimes, in line with section 14, “enabling” terrorism casts a problematically wide net, since it could be applied to a range of innocent actors. A standard of aiding and abetting, as spelled out in section 14, should be the minimum threshold for being charged as an accomplice to the crime.

Additionally, while most of the provisions of section 7 require that an action “seriously” interfere with, disrupt or damage a vital service, section 7(1)(b)(i) omits the word “seriously”, allowing for the higher penalties to attach to any interference with, disruption to or damage to a public utility service or communication system. Given the severity of the section 7 penalty, it should be reserved for serious cases.

Section 13, which contains provisions for the protection of women, is also troublingly overbroad. Although many aspects of the section are reasonable, such as prohibitions on threatening sexual acts or distributing photographs of women engaged in sexually explicit conduct without their consent, the language also forbids any communication which harms the reputation of a woman, meaning the provision effectively acts as a criminal defamation law, with a penalty of up to one year imprisonment as well as an unspecified fine.

International standards stipulate that defamation should be a civil, rather than a criminal offence. According to a General Comment issued in September 2011 by the UN Human Rights Committee, the official body responsible for overseeing States’ compliance with their ICCPR obligations:

The Centre for Law and Democracy is a non-profit human rights organisation working internationally to provide legal expertise on foundational rights for democracy

States parties should consider the decriminalization of defamation and, in any case, the application of the criminal law should only be countenanced in the most serious of cases and imprisonment is never an appropriate penalty.⁸

Given that Pakistan already criminalises defamation under section 499 of the Pakistan Penal Code Act, 1908, there is certainly no reason to introduce an additional criminal defamation standard for cyber offences. Many democracies, including East Timor, Georgia, Ghana, Sri Lanka, the United Kingdom and the United States, have repealed their criminal defamation laws while others have done away with the possibility of imprisonment for defamation.

The prohibition in section 13 against distorting the face of a woman in any photograph is also problematic since these types of modifications are routinely done for innocuous reasons, including to protect the identity or privacy of individuals.

Recommendations:

- Section 7(1) should not apply to threats.
- Section 7(1)(b)(i) should only apply to serious interferences, disruptions or damage.
- Section 7(1)(b)(vii), which criminalises enabling terrorism, should be removed.
- Section 13 should not apply to defamatory statements or to distorting the face of a woman.

5. Enforcement and Procedural Mechanisms

It is notable that, compared to the initial draft which was published in January 2014, the procedural protections contained in the draft Act have been significantly improved. The rights of suspects as well as third-parties are explicitly spelled out. The Federal Investigation Agency, which will bear primary responsibility for enforcement of the draft Act, is subject to rigorous judicial scrutiny over the use of their new powers. Officers who investigate crimes, as well as judges who hear issues related to its enforcement, are required to undergo specialised training in digital issues. These are very positive measures. However, section 50 of the draft Act specifically exempts intelligence agencies from these safeguards, providing no guidance as to how, or whether, their powers in this area will be checked. This is a troubling omission.

⁸ General Comment No. 34, 12 September 2011, CCPR/C/GC/34, para. 47.

A significant problem with the enforcement mechanisms in the draft Act is in section 31, which requires service providers to retain all traffic data “within its existing or required technical capability” for a period of ninety days. Pakistan is not alone in considering these types of data retention measures. Similar procedures have been drafted elsewhere, most notably in the European Union, under the Data Retention Directive.⁹ However, these rules have also been subject to significant criticism.¹⁰ Several EU States are refusing to implement the Data Retention Directive, including Germany and Sweden, and courts in the Czech Republic, Cyprus, Bulgaria and Romania have found its provisions to be unconstitutional. In December 2013, Pedro Cruz Villalón, an Advocate General at the European Court of Justice, issued an opinion that the Directive was incompatible with the Charter of Fundamental Rights of the European Union.¹¹ The Directive has also been challenged in the European Court of Justice, which is due to rule on its legitimacy later this year. Australia's government proposed a data retention scheme, but shelved the idea in 2013 in the face of significant opposition.¹² The United States Congress proposed laws which included data retention components in 2009 and 2011, but neither were passed.¹³

There are two main arguments against imposing mandatory data retention schemes. The first is that such a sweeping surveillance measure exerts a significant chilling effect on expression. The importance of protecting communications against undue surveillance has been recognised by the UN Special Rapporteur on Freedom of Opinion and Expression:

States cannot ensure that individuals are able to freely seek and receive information or express themselves without respecting, protecting and promoting their right to privacy.... Without adequate legislation and legal standards to ensure the privacy, security and anonymity of communications, journalists, human rights defenders and whistleblowers, for example, cannot be assured that their communications will not be subject to States' scrutiny.¹⁴

Even if the data logs are destroyed after 90 days, the mere fact of their being recorded can be expected to chill the expressive discourse by undermining users' confidence in the confidentiality of their communications. Moreover, although the draft Act limits when and how the Federal Investigation Agency can access this data,

⁹ Directive 2006/24/EC.

¹⁰ See, for example, Centre for Law and Democracy, European Union: Analysis of the Data Retention Directive, 2013. Available at: <http://www.law-democracy.org/live/european-union-data-retention-directive-not-justifiable/>.

¹¹ Case C-293/12. Full decision available at: <http://curia.europa.eu/juris/documents.jsf?num=C-293/12>.

¹² See <https://www.eff.org/deeplinks/2013/06/mandatory-data-retention-defeated-australia-now>.

¹³ See <https://www.eff.org/issues/mandatory-data-retention/us>.

¹⁴ Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 17 April 2013, UN Doc. A/HRC/23/40, para. 79.

it is significant that no such limits are imposed on the intelligence agencies listed in section 50.

Measures which exert an indirect chilling effect on free speech represent interferences with the right to freedom of expression, and this is acknowledged explicitly in Article 13(3) of the *American Convention on Human Rights*:

The right of expression may not be restricted by indirect methods or means, such as the abuse of government or private controls over newsprint, radio broadcasting frequencies, or equipment used in the dissemination of information, or by any other means tending to impede the communication and circulation of ideas and opinions.¹⁵

The second major argument against data retention schemes is that they are fundamentally insecure. Despite any safeguards that telecommunications providers may take, such rich data pools present a tempting target for hackers. For example, in 2006, traffic data from 17 million users was stolen from Deutsche Telekom, a German telecommunications giant. In response, Deutsche Telekom illegally used its own traffic data to spy on 60 individuals suspected of being involved in the theft, including journalists.¹⁶ In July 2012, when the Australian government announced that it was considering proposals to require Australian ISPs to retain data from their users, the hacker collective Anonymous responded by promptly hacking into the database of a major ISP.¹⁷

While the desire for effective online surveillance is understandable, broad data retention schemes are an unacceptable invasion of privacy, and severely undermine freedom of expression online.

Recommendations:

- The draft Act should impose reasonable checks on the powers of intelligence agencies with regards to investigation and surveillance.
- Section 31, which provides for mandatory data retention, should be removed.

¹⁵ Adopted 22 November 1969, O.A.S. Treaty Series No. 36, entered into force 18 July 1978.

¹⁶ German Working Group on Data Retention, *There is no secure data*. Available at: http://wiki.vorratsdatenspeicherung.de/images/Heft_-_es_gibt_keine_sicheren_daten_en.pdf.

¹⁷ Joel Falconer, "Anonymous hacks Australian ISP AAPT to demonstrate data retention problems", The Next Web, 26 July 2012. Available at: <http://thenextweb.com/au/2012/07/26/anonymous-hacks-australian-isp-aapt-to-demonstrate-data-retention-problems/>.