## Introduction

Internet and technology have been recognized as great enablers in creating new opportunities for business, paving way for a thriving culture of entrepreneurship and innovation (also social); breaking down literacy barriers; facilitating the democratization of systems; connecting people and societies, and providing platforms for dialogue and exchange of views between citizens around the world. Knowledge, information as well as the ability to communicate lies at one's fingertips now like never before.

With the arrival of smartphones, even a mobile phone is now a computing device. According to the Pakistan Telecommunication Authority's (PTA) July 2015 report, the total teledensity in Pakistan stands at 63.6%. There are 116,431,523 annual cellular subscribers. 3G/4G Subscribers stand at: 14,614,411. The figures for broadband subscribers by technology are 18,001,252 (Mobile BB: 14,614,411).

While much good has come from the easy access and spread of technology, this space is not free of dangers or criminal activity. Where there are positive, legal uses of technology, there are negative and illegal uses as well. Compromised email or social media accounts are a common occurrence that plague the average Internet and technology user, leading in turn to other misuses and crimes such as data and identity theft. Such activities impact the average user, businesses and the government.

Due to the nature of this medium, often existing laws are found wanting to cover the wide spectrum of crimes unique to this medium, which necessitates a law of a very specific nature – both in terms of the offences it creates and the procedures to deal with them. There is no disagreement over the fact that a cybercrime law is the need of the hour. However, given that there is still relatively low computer and technology literacy in the country, a law that deals with crimes needs to be carefully crafted. While it should serve the rightful purpose of curtailing criminal activity, it should not place the fear of technology among a people still embracing and learning to use this medium. Neither should it treat every user as a potential criminal.

## The Prevention of Electronic Crimes Bill 2015

**Process:**

The biggest failing has been the process – or lack of –as far as the drafting of the Prevention of Electronic Crimes Bill 2015 is concerned. It has taken place behind closed doors, with the exclusion of members of opposition, and without any public or expert input.

Despite repeated attempts by members of opposition, industry and civil society groups to provide input and make this a public and transparent process, all such efforts have been thwarted. Repeated requests for meetings and hearings have been denied. Meetings, to which members of opposition were invited, have been scheduled at a day's notice at times.

On September 17, 2015, the National Assembly's Standing Committee on Information Technology and Telecommunications approved the government's proposed Prevention of Electronic Crimes Bill 2015, for a second time. An earlier version was approved in April 16, 2015. Both versions were approved despite reservations expressed by members of opposition part of the NA Standing Committee on IT.

Despite all the verbal and written input provided, next to nothing has been accommodated in the latest approved version of the bill. Not only was the bill once again approved with much haste, but a copy of the bill was not even placed before the members of the NA Standing Committee on IT to review before casting a vote.[1]

**Content:**

The fundamental flaw with the government's proposed Prevention of Electronic Crimes Bill is that it tries to kill too many birds with one stone – and disproportionately at that. There is no distinction between telecom offences, cybercrimes and social ills – they have all been packed into one law and criminalized.

The proposed bill will function as a **gag law** should it come to pass in its current form. It prescribes blanket censorship, curtails political speech, and seeks to control dissenting views, debate and dialogue, sanctioned particularly under **Section 34.** This section is a copy paste of Article 19 of the Constitution and the Pakistan Telecommunications Authority (PTA) is directly empowered to interpret the exclusion clauses and remove content from the Internet or any information system as it deems fit.

Much is left to the **discretion** of authorized officers, authorities and agencies, and the federal government. **Overbroad powers** have been given to regulatory and investigation bodies without any checks and balances or accountability mechanisms. For instance, Section 32 gives an authorized officer the power to ask someone to divulge encryption keys or passwords. This

[1] http://bolobhi.org/resources/press-kit/pecb2015-the-story-so-far/

forces an individual - and by default those connected to him her – to divulge and provide access to private data beyond what may be necessary or within the scope of the investigation. It also poses a risk to companies who are required to sign confidentiality agreements or MoUs for business.

**Judicial oversight,** with the exception of requiring warrants for search and seizure, remains absent in the proposed law. Data and information are everything today. Authorities and officers should not get easy access to it unless legitimately required and as sanctioned by court.

The proposed bill does not distinguish between innocent people and criminals. In turn, it prescribes heavy penalties in the form of jail terms and fines.

Whistle-blowers, white-hat hackers etc. also run the risk of being treated as common criminals.

Loosely worded sections leave too much room for interpretation and misinterpretation, widening the window for misuse and likelihood of the provisions of this bill being used for score-settling rather than addressing criminal activity.

## Major Concerns

Some of the most problematic sections of the bill are as follows:

**Sections that impact speech and expression:**

**Section 9: Glorification of an offence and hate speech** criminalizes even the 'preparation' of information even if it is not disseminated. To advocate for a person wrongly accused or convicted of a crime or terrorism charges would not just be illegal but punishable by five years in prison or with a fine up to ten million rupees or both. Critiques of judgments – which are commonplace - could also be criminalized, as would be any voices highlighting miscarriage of justice could be misconstrued as 'glorifying' an accused or convicted person.

**Section 18: Natural Dignity of a Person –** criminalizes the act of exhibiting, displaying or transmitting 'false information,' which is 'likely' to 'harm or intimidate the reputation or privacy of a natural person.' While this doesn't apply to anything aired on television, it applies to everything uploaded and shared online. Political expression and satire is not exempted. Some examples how this can be misapplied:

The person who uploaded Rehman Malik's video of boarding a flight late would be jailed for it. In fact he did lose his job and was charged under the Maintenance of Public Order. PTI activist Qazi Jalal was charged under Section 36 & 37 of the ETO for a tweet in which he alleged a judge's son-in-law was deriving benefits due to his in-laws' position. He included a wedding card in his tweet to corroborate the person in question was actually the son-in-law. In Turkey, a man is facing a two-year jail term for sharing a meme comparing Erdogan and Gollum – character from the Lord Of The Rings Trilogy. Would the same happen to person who

created/shared the Nawaz Sharif & Shrek meme? And any other form of political expression, satire or citizen journalism will be construed as harm to reputation. Either people will start to self-censor – as is now rampant on channels and do a great degree in print – or people will be facing jail terms.

**Section 21: Cyber Stalking –** The following acts are criminalized under this section: (a) 'communicate obscene, vulgar, contemptuous and indecent information;' (b) 'any suggestion or proposal of an obscene nature;' (c) threaten to commit any illegal or immoral act; (d) take a picture of any person and display or distribute without his consent or knowledge in a manner that harms the person.

Whose definition of 'obscene, vulgar, contemptuous, indecent, obscene and immoral' would be applied? What about pictures taken without permission if they are covering crowds at public events? Or those pictures zeroing in on public/known figures attending rallies/congregations by banned organizations, in an attempt to call them out or hold them accountable for it? This carries a jail term of up to three years.

**Section 34: Powers to manage on-line information –** The PTA is given policing powers: 'empowered to manage information and issue directions for removal or blocking of access of any information through any information system.' Moreover 'the Authority may direct any service provider to remove any information or block access to such information if it considers it necessary' as per the exceptions listed out in Article 19.

This clause gives the government/PTA unfettered powers to block access or remove speech not only on the Internet but transmitted through any device. It is a copy-paste of Article 19, allowing the PTA to interpret how the exclusions are to be applied. Just like PEMRA issues directives to the electronic television channels, PTA would do the same to ISPs.

In the past, Beyghairat Brigade's video critical of the army was blocked. Shia killings, a website that documents sectarian killings, stands blocked. IMDB, a movie database was blocked because there was a review and link to a documentary on Balochistan on it. Instagram was blocked on the pretext of there being pornographic material available on it.

All the alternate views found on the Mina tragedy that emerged on social media would stand blocked. No dissenting view would be available on Balochistan. As it is, several sites stand blocked on the pretext of them being 'anti-state.' Any commentary on religion or a view other one particular sect's interpretation could be blocked in the name of protecting 'the glory of Islam.' The Internet in Pakistan will become an extended version of PTV: all dissenting views would be controlled and only the state version.

In Sections 18, 21 and 34 listed above, PTA is given sole discretion over content. In the case of Sections 18 and 21, while they are non-cognizable and compoundable, the 'aggrieved' can apply directly to PTA for 'removal or destruction of, or blocking access of such information' and 'the Authority may on receipt of such application may take such measures as deemed appropriate for removal or destruction of, or blocking access to, such information.' In Section 34, no one has to apply to PTA; it can act unilaterally and issue instructions as it deems fit.

**Sections that put privacy at risk**

**28. Expedited preservation and acquisition of data** – An 'authorized officer' may write to a person in control of an information system and require him/her to provide data or order that specified data be preserved up to 90 days. It is after this is done that the authorized officer must bring this to the court's attention within 24 hours. So post-PECB, we will be receiving written orders from not even the agency but an officer, to hand over data. 24 hours is long enough a period to misuse the powers given.

**29: Retention of data –** a service provider (i.e. ISP) is required to retain data (of its customers) up to a year and provide it to the investigation agency or authorized officer as and when notified by the Authority to do so. Our entire digital footprint – what we accessed, who we communicated with and the specific contents – would be on offer.

**32: Powers of an authorized officer** Sub-section (g) requires the disclosure of encryption keys (passwords etc.), forces an individual to divulge and provide access to private data beyond what may be necessary or within the scope of the investigation. It also poses a risk to companies who are required to sign confidentiality agreements or MoUs for business. The 'authorized officer' is empowered to make this request/notify person without seeking court approval.

**33: Dealing with seized data** - Currently this has been left to the discretion of the federal government and its rule-making powers, while the procedure should clearly be stipulated under this bill (as it was in the stakeholder version). What would happen to an information system or device once it is seized? Who will ensure the information and data in the device or system is not browsed through – or damaged/altered/deleted. While for investigation purposes, a specific file may be required, however the ability to access other files would also exist once the device is in possession. One person's device/information system also provides access to thousands of other people, who fall well beyond the scope of investigation.

**36. Real-time collection and recording of information –** Based on an application by an authorized officer, 'if a Court is satisfied that the content or any information is reasonably required for the purposed of a specific criminal investigation, the court may order with respect to information held by or passing through a service provider, to a designated agency…having the capability to collect real time information, to collect or record such information in coordination with the investigation agency.' For a period of seven days, real-time activity will be recorded as sanctioned by court. Everything as it is being typed and transmitted would be recorded and visible. There is no mention of the capability and methods that will be used to do this – how invasive they would be. The same instruments used to record for seven days can (and most likely will) be used for continued and selective and/or broad-based surveillance.

**Section 37: International Cooperation**. This section gives the federal government unbridled powers to share information with international governments/agencies without any oversight. Again, in the absence of privacy and data protection legislation, it becomes all the more essential a process be formulated and stipulated under this law that creates a framework within which data of Pakistani citizens is to be acquired and exchanged with foreign companies and governments.

While in the revised version of the bill Section 31: Warrant for content data, has been added, whether or not it would apply to the above sections and how, is ambiguous. Section 31 reads: 'upon the application by an authorized officer that demonstrates to the satisfaction of the court that there exist reasonable grounds to believe that the content data stored in an information system is reasonably required…the Court may, after recording reasons, order that a person in control of the information system or data, to provide such data or access to the authorized officer.'

Section 31 pertains to the 'disclosure of content data.' It speaks nothing of data other than content data. In this bill, data is defined as 'traffic data and content data.' Moreover other forms of 'data' are covered under other definitions. Information for instance is defined as: 'text, message, data, voice, sound, database, video, signals, software, computer programs, any form of intelligence as defined under the PTA (Reorganization Act 1996 and codes including object code and source code.'

So while a warrant would be required for disclosure of 'content data,' there is no procedure nor oversight prescribed for the acquisition, disclosure, retention, preservation or handling of traffic data – which is also identifiable data (i.e. can reveal a person's location and identity. Nor does this exist for information – the definition for which contains nearly all forms of data. Moreover Section 31 deals with a person in control of the information system or data, and not service providers or those storing data on behalf of others. Therefore the token warrant for content data hardly serves as a safeguard for the above-listed sections, which give sweeping powers over - and intrusive access - to everyone's communication and data. And there is no data protection or privacy legislation in Pakistan.

**Other Sections:**

Definition of ***offence*** makes children as young as 13 culpable under this bill. These offences differ in nature to offences listed out under the PPC. No distinction is made in terms of the gravity of an offence and how, if committed by a minor, the treatment/punishment would vary.

Definition of ***unauthorized access*** and Sections 3-4 & 6-7 do not create an exception for whistleblowers, white-hat hackers and hobbyists who, under this law would land up in jail for their activities, which are not categorized as criminal otherwise. Journalists too would be penalized for investigative reports. In an environment where everything is classified and even legitimate right to information requests denied, tip offs and leaked documents in public interest would lead to jail terms.

**Section 15: Unauthorised issuance of SIM cards etc.** is a telecom offence that should be dealt with under the PTA Act. Telecom already is a heavily regulated sector. Moreover, imposing criminal penalties conflicts with intermediary liability protection extended through Section 35.

**Section 22: Spamming,** the transmission of 'unsolicited information' without the 'express permission of the recipient' has been criminalized. It is unclear as to how one should acquire express permission. This will disrupt the very nature of public messaging relied on not only by

businesses but political parties, educational institutes and other organizations. There is no need to include this in this law, or criminalize the act. There are other ways of dealing with this, particularly through the existing telecommunications regulatory regime or, through tools available in mobile phones and email inboxes. People should not be jailed for what is an irritant.

**Section 27: No warrant, search, seizure or other power not provided for in the Act:** too much if left to the discretion of government authorities, no judicial oversight, especially data-related sections.

**Section 42: Appeal.** An appeal should not be limited to only the final judgment of court and the provision for an appeal to be made before a High Court should exist.

## Case Studies: Abuse of Law

### Pakistan: Abuse of authority by investigating and law-enforcement agencies

Faisal Chohan was a young CEO of an Islamabad-based company. Back in 2006, his office was raided on the 'suspicion' that his company was involved in VoIP activities. Servers, routers, equipment were confiscated. He was charged under Sections 36 and 37 of the Electronic Transactions Ordinance and thrown behind bars in Adiala where he spent 13 days, even though he was innocent and his company's IP address had been wrongly matched with the actual offender's, as it later turned out and was admitted to by PTA.[2]

Faisal's was a classic case of excess and misuse of executive authority (PTA & FIA). It highlights in particular the bureaucratic and judicial hurdles faced (formal withdrawal of charges, multiple rejections of bail application). This illustrates not only the legal and procedural issues but prevalent mindset in our institutions which hampers justice.

More recently, Qazi Jalal, a PTI activist was charged under Sections 36 & 37 of the ETO and arrested for slandering a member of the judiciary in tweets he sent out[3].

### Turkey: Criminalizing criticism & critique of the head of state

Turkish President Tayyip Erdoğan himself as well as members of his family filed several cases against journalists over alleged insults. [4] Censorship and repression of free speech has increased under his rule in Turkey, and political satirists, cartoonists, journalists have been dealt with by a heavy hand. In current cases, a man is facing charges for sharing a meme comparing Erdogan to Gollum, a fictional character existing in Tolkien's book trilogy, "Lord of the Rings."[5] [6]

### Abu Dhabi: Charged for posting a picture of a badly-parked car on Facebook

An Australian woman in Abu Dhabi was jailed for posting a picture on Facebook. Her crime was uploading a picture of a car without a disability sticker parked in a disabled parking space in her apartment block. She was found guilty of "writing bad words on social media about a person" and was told she would be deported.[7]

[2] http://wheelofjustice.blogspot.com/
[3] http://www.dawn.com/news/1215966
[4] http://www.todayszaman.com/national_one-third-of-days-court-calendar-concerns-insults-to-erdogan-family_407648.html
[5] http://www.news.com.au/finance/business/media/man-facing-jail-over-gollum-meme/news-story/3e862063b53c29fa61dd9658dd2dbc17
[6] http://www.bbc.com/news/world-europe-34979249
[7] http://mashable.com/2015/07/13/australian-abu-dhabi-facebook/

**UAE: Heavy fine for swearing online**

In 2014, a new cybercrime law was passed in the UAE which made online verbal insults a criminal offense. This law was made prominent in a case in June 2015, where a man was fined $250,000 for swearing at his colleague via Whatsapp.[8] This law impact expats as well.[9] Under the same law, expats can also be charged with a criminal offence if they possess a photo taken without the subject's consent.[10] The law also applies if a person is possession of a photo on their phone, even if they have not shared it publicly.

**India: Girl arrested for Facebook status questioning shutdown of city for Bal Thackeray's funeral**

The police arrested a 21-year-old girl for questioning the total shutdown in the city for Bal Thackeray's funeral on her Facebook account. Another girl who 'liked' the comment was also arrested. The two were booked under Section 295 (a) of the IPC (for hurting religious sentiments) and Section 64 (a) of the Information Technology Act, 2000. Though the girl withdrew her comment and apologized, a mob of some 2000 Shiv Sena workers attacked and ransacked her uncle's orthopaedic clinic at Palghar, north of Mumbai.[11]

Other prominent cases of abuse include the arrest of a teenage boy arrested for sharing a Facebook post.[12] In another, a university professor who was arrested on the basis of forwarding an email satirizing a politician.[13] Not only was he charged under Section 66(a) but he was also charged under Section 114, 500, and 509 of the ITC Act.[14] Another man was arrested for drawing cartoons of politicians. [15]

**United Kingdom: Man arrested for charging phone on the train**

A man was arrested in London for charging his phone on a train while in transit.[16] A community police officer on the London Underground arrested him for using an electric socket on the train,

[8] http://www.bbc.com/news/world-middle-east-33152898
[9] http://www.emirates247.com/news/emirates/new-uae-online-law-dh250-000-fine-for-swearing-on-whatsapp-2015-06-16-1.593945
[10] http://www.thenational.ae/uae/tough-uae-social-media-law-could-see-expats-deported-for-saving-someones-photo
[11] http://timesofindia.indiatimes.com/india/21-year-old-girl-held-for-Facebook-post-questioning-Mumbais-Bal-Thackeray-shutdown/articleshow/17276979.cms
[12] http://timesofindia.indiatimes.com/city/bareilly/Class11-student-sent-to-jail-for-Facebook-post-against-UP-minister-Azam-Khan/articleshow/46600144.cms
[13] http://www.hindustantimes.com/india/professor-arrested-for-poking-fun-at-mamata/story-OmV4FhEop4XaRP13gZdI1H.html
[14] http://www.ndtv.com/india-news/west-bengal-professor-attacked-4-arrested-released-on-bail-476645
[15] http://www.nationalturk.com/en/man-arrested-in-india-for-posting-cartoons-of-pm-others-on-fb-33370
[16] http://www.bbc.co.uk/newsbeat/article/33510792/a-man-was-arrested-for-charging-his-phone-on-a-train-why

accusing him of stealing electricity which is loosely covered under the offence of abstracting of electricity under the Theft Act of 1968.[17]

**Bangladesh: Student charged with sedition for a Facebook comment about Prime Minister**

A 29-year-old PhD student was charged with contempt of court in Dhaka and sentenced to six months in jail for failing to appear before the High Court to explain why he should not face trial for posting a derogatory comment about Prime Minister Sheikh Hasina on his private Facebook wall.[18]

**Thailand: Woman arrested for criticizing the junta**

Online regulation is abused to silence political dissent in Thailand, where it is a crime to speak against the monarchy under a strict lèse-majesté law. The law applies to spoken and verbal discourse, which also applies to anything written and transmitted online. A woman arrested for criticizing the military junta in a Facebook post.[19] Her Facebook posts were investigated, and she was charged with sedition.[20]

**Malaysia: Student activist arrested for criticizing the government**

Ali Abdul Jalil, a student activist, was arrested and held in Selangor state, Malaysia, after posting remarks critical of the Malaysian government on his social media page.[21] He was repeatedly arrested, released, and rearrested multiple times for criticizing the monarchy, and speaking against the state. [22] In a similar case, two men were arrested for allegedly slandering the royal family.

[17] http://www.theguardian.com/technology/2015/jul/13/man-arrested-charging-iphone-london-overground-train
[18] http://www.theaustralian.com.au/higher-education/bangladeshi-student-fears-death-penalty-for-facebook-comment/story-e6frgcjx-1226240283288
[19] http://www.bbc.com/news/world-asia-35113796
[20] http://www.bangkokpost.com/news/crime/796496/single-mother-jailed-7-years-for-facebook-post
[21] http://forcechange.com/133435/free-student-arrested-for-social-media-posts/
[22] http://www.themalaymailonline.com/malaysia/article/re-arrested-a-third-time-activist-marks-20th-day-in-jail-for-facebook-slur

## A view from around the world

Two international conventions and covenants become relevant in a discussion on the cybercrime bill. The International Covenant on Civil Political Rights (ICCPR)[23], and the Council of Europe's Budapest Convention. Pakistan has signed and ratified the ICCPR, a human rights framework.

The Budapest Convention on Cybercrime[24] outlines the types of offences cybercrime laws cover and the procedures they should list. Typically the offences relate to illegal access, illegal interference with systems, identity theft, fraud, child pornography. Fifty countries are signatory to this convention and 47 have ratified it. Pakistan is not one of them.

World over, there exist examples of either enabling legislation that protect citizens' basic rights, or more recent examples where overbroad legislation has been challenged in court and courts have struck down provisions.

**Brazil:** The Brazilian Civil Rights Framework for the Internet (*Marco Civil da Internet,* or MCI) is a comprehensive piece of legislation that upholds basic rights on the Internet, outlines guarantees and duties of users; and prescribes guidelines for the state and when and how it may act. This was approved in March 2014 by the Brazilian Congress and by the Senate in April 2014.

**Philippines:** In 2014, the Magna Carta for Internet Freedom was filed as an attempt to repeal the cybercrime law.[25] This was the first time a bill was crowdsourced in the Philippines. Also, the same year, Philippines Supreme Court struck down three clauses from the cybercrime law, Sections 4 c)(3) which pertains to unsolicited commercial communications; 12 which pertains to real-time collection of traffic data; and 19 which pertains to restricting or blocking access to computer data. Technology activists were successful in making their case before court that even traffic data was identifiable data and therefore its collection infringed privacy and opened doors to mass surveillance. It also struck down a provision of the law that gives the state power to block content online without a court order.

**India:** In March 2015, the Indian Supreme Court struck down 66A, a provision of the Indian IT Act "that allowed people to be arrested for 'annoying' or 'offensive' content, including Facebook posts." As reported: "66A was found to be vague and inconsistent with the 8 (constitutionally) permissible grounds for restriction of freedom of expression." This came after a lengthy two-year long campaign and many abuses of the law, which landed people in jail for status updates and

[23] http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx
[24] http://www.cto.int/media/events/pst-ev/2013/Cybersecurity/Alexander%20Seger-Budapest%20Convention%20on%20Cybercrime.pdf
[25] https://www.senate.gov.ph/lisdata/1446312119!.pdf

emails.[26] Critics and activists opposed Section 66A for obstruction of free speech and citizen's right to know, and the section was heavily abused by the police.[27]

**USA:** In June 2015, "The Senate passed the USA Freedom Act without any amendments. The bill prescribes "an end to mass collection of Americans' phone records by the NSA, restore some expired powers to security agencies, place record storage in private companies' hands, create a public-interest advocate for the secret FISA court that oversees surveillance programs, and require the court to notify Congress when it reinterprets law."[28]

The Senate head of security was quoted as saying: "I don't believe that the threat level has dropped to a point where we can remove some of the tools – if anything, the threat level has gotten higher, and you would think we'd be talking about an expansion of tools. But I accept the fact that this debate has gotten to a point where a bulk data storage capacity within the government is not going to be continued long term."[29]

Conservatives in America claimed that oversight and reforms are equivalent to supporting terrorists. However, America finally decided not to be held hostage to such fear-mongering that ushered in the Patriot Act, Guantanamo, and blanket NSA surveillance. Yet the USA Freedom Act is a step forward in the right direction though much more needs to be done to reverse the surveillance regime.

As far as speech goes, First Amendment to the Bill of Rights guarantees citizens freedom of expression.[30] The Amendment reads, "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."[31] There is tremendous case law on this and it is fiercely protected.

**EU:** In June 2015, the European Council approved its version of the General Data Protection Regulation (GDPR). This will create a unified data protection regime for 28 EU states. The next stage is for the European Commission, European Parliament and European Council (each has its own preferred version of the regulation) to jointly agree on the final text of the regulation. These discussions will commence officially on June 24, 2015, and are currently scheduled to produce the final version of the GDPR by December 2015.[32]

[26] http://www.theguardian.com/world/2015/mar/24/india-supreme-court-strikes-down-internet-censorship-law
[27] http://www.hindustantimes.com/india/facebook-trouble-10-cases-of-arrests-under-sec-66a-of-it-act/story-4xKp9EJjR6YoyrC2rUUMDN.html
[28] http://www.theguardian.com/us-news/live/2015/jun/02/senate-nsa-surveillance-usa-freedom-act-congress-live
[29] http://www.theguardian.com/world/2015/jun/01/mitch-mcconnell-limit-transparency-usa-freedom-act
[30] http://constitution.findlaw.com/amendment1.html
[31] http://www.ala.org/advocacy/intfreedom/censorshipfirstamendmentissues/courtcases
[32] http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf

**UK:** In July, a UK High Court ruled that the Data Retention and Investigatory Powers Act was unconstitutional. Two UK Members of Parliament had contested the legislation on the grounds that it violated rights and privacy. In particular, it was found to be inconsistent with EU laws and "incompatible with article eight of the European convention on human rights, the right to respect for private and family life, and articles seven and eight of the EU charter of fundamental rights, respect for private and family life and protection of personal data." The government was given until March 2016 to come up with a new law. That process has been underway and a joint committee was set up to review the bill and issue a call for submissions so an informed decision is made.

…

There are many other relevant conventions, guidelines and principles that should be reviewed while drafting a cybercrime bill.

Listed below are the most relevant ones:

- Convention for the Protection of Individuals with regard to Automatic Processing of Data
- European Convention on Human Rights
- Johannesburg Principles on National Security, Freedom of Expression and Access to Information
- Manila Principles
- International Principles on the Application of Human Rights to Communications Surveillance
- UN Guiding Principles on Business and Human Rights
- Global Network Initiatives Principles on Free Expression and Privacy

## Recommendations

First and foremost, Pakistan needs to enact good data protection and privacy legislation. At the same time we need **enabling legislation** for Article 19, further strengthening citizens' right to speech.

As for the Prevention of Electronic Crimes Bill, it needs to be revisited and if not completely redrafted then heavily **amended** to bring it line with a constitutional framework that **safeguards rights.** This should be done through an open, transparent and consultative process. Citizens' right to privacy, speech and due process need to be ensured.

Speech-related offences and those that pertain to the telecom sector should be omitted from this bill; only computer/medium specific crimes should remain.

The **age** distinguishing a minor and an adult should be 18.

**'Malicious intent'** should be added to all sections on offences to establish mens rea.

**Warrants** should be required for not only search and seizure, but for all offences. An officer should have to provide reasoning before court as to why access to a person's data, device or to the accused himself/herself is necessary. This becomes all the more necessary in the absence of data protection and privacy legislation.

**Procedures** should be defined under this law rather than left up to the rule-making powers of the government. Moreover, the rule-making powers of the government should also be subjected to public scrutiny – all proposed rules should go through the public eye before coming into effect.

**Penalties** should exist for service providers and investigation officers who step beyond the scope of duty and misuse information they may gain access to – especially in the absence of privacy and data protection legislation.

**Cooperation** with foreign governments and entities – and on what terms – should be subjected to a well-defined procedure stipulated under this law.
The data of Pakistani citizens should not be readily shared or handed over -protections and procedures need to be in place. Again, especially since data protection and privacy laws do not exist.

**Conclusion:**

Given that there is still relatively low computer and technology literacy in the country, a law that deals with crimes needs to be carefully crafted. While it should serve the rightful purpose of curtailing criminal activity, it should not place the fear of technology among a people still embracing and learning to use this medium. Neither should it treat every user as a potential criminal.

The bill, in its current form, is likely to inculcate the fear of technology, which would negatively impact the growth the ICT sector has witnessed or the manner in which people have embraced technology - for the good.

Due to the nature of this medium, often existing laws are found wanting to cover the wide spectrum of crimes unique to this medium, which necessitates a law of a very specific nature – both in terms of the offences it creates and the procedures to deal with them. There is no disagreement over the fact that a cybercrime law is the need of the hour. However, given that there is still relatively low computer and technology literacy in the country, a law that deals with crimes needs to be carefully crafted.

Any cyber crime bill introduced should be in line with a constitutional framework that safeguards rights. This should be done through an open, transparent and consultative process. Citizens' right to privacy, speech and due process need to be ensured.