Proposed Cybercrime Law: Reason to Worry

A Presentation by Bolo Bhi
I'M BRINGIN' PECO BACK

#ProposedCyberCrimeLaw
PECO (Pakistan Electronic Crime Ordinance) was promulgated by Musharraf in 2007. Since it was an ordinance, it lapsed in 2009. There was huge uproar against it because innocent people were charged and framed. It gave excessive powers to FIA (Federal Investigation Agency), which were abused.

In this timeline you will find the different versions of the laws and reactions and analyses of them:

http://bolobhi.org/resources/timelines/tracking-cyber-crime-legislation/

The government’s proposed cybercrime bill is akin to resurrecting PECO - if not introducing something far worse.
DEAR MOITT,

# CYBERCRIME BILL
NON INCLUSION
STAKEHOLDERS
INDUSTRY
CIVIL SOCIETY

ہر ایک بات پر کہتے ہو تھے کہ تو کیا ہے،
تم ہی کہو کہ یہ اندہ اگتگو کیا ہے
CONTEXT

Once PECO lapsed, there were efforts to revive it and introduce PECO as an Act. That is when the industry really got involved and started drafting their own version. ISPAK (Internet Service Providers Association) and P@SHA (Pakistan Software Houses Association) led this initiative. Last year, there were meetings at the Ministry of IT & Telecommunications which members of P@SHA & ISPAK attended to finalize the industry stakeholder draft (please note though no civil society organization or members were privy to these meetings or drafts). This was then sent to the Cabinet Division. From there it emerged earlier this year with modifications.

Since then, despite efforts to become a part of the redrafting process, industry, civil society even members of opposition have been excluded from the drafting process. After this, a sub-committee was formed to work on the bill further. Bolo Bhi held consultations with industry and civil society members, and technical experts - we were also in touch with the original drafters of this law.

See:
http://bolobhi.org/cybercrime-bill-must-not-approved-current-form-2/
This is the government’s plan, basically...
The Red Flag Has Been Raised

The proposed bill is everybody’s problem. It impacts end users as much as it will impact business and the media. So long as you own a technology device, this impacts you. Here’s how:
(x) "service provider" includes-

iv) any person who provides premises from where or facilities through which the public in general may access information systems and the internet such as cyber cafes;
As per the “new” definition of service providers...

→ THEY ARE NO LONGER LIMITED TO TELCOS AND ISPS BUT ALSO INCLUDE:

→ Any place that provides Internet access to the general public. So, what’s the problem? They will be required to retain traffic data...
Section 26: Retention of Traffic Data

26. **Retention of traffic data.**---(1) A service provider shall, within its existing or required technical capability, retain its traffic data for a **minimum period of ninety days** or such period as the Authority may notify from time to time and provide that data to the special investigating agency or the investigating officer whenever so required.

Under this law, service providers are no longer just telcos and ISPs but places such as T2F, Kuch Khaas, The Nest; restaurants and cafes such as Espresso, Gloria Jeans etc; malls and offices etc. Basically any place that offers access to the Internet.

This places an unrealistic and impossible burden on businesses who are neither equipped nor should be to perform such a function, also increasing significantly, the cost of doing business.
Furthermore, subsection (3) of Section 26 not only mandates service providers retain data but also criminalizes, it seems, a person/service provider who does not retain traffic data.

3) Any person who contravenes the provisions of this section shall be punished with imprisonment for a term which may extend to six months or with fine which may extend to or with both.
Section 8: Cyber Terrorism

This has a very different meaning than what we take cyber terrorism to mean. This is defined as follows:

8. **Cyber terrorism.** –Whoever commits or threatens to commit any of the offences **under sections 5 and 7** where-

(a) the use **or threat** is designed to coerce, intimidate, overawe or create a sense of fear, panic or insecurity in the Government or the public or a section of the public or community or sect or create a sense of fear or insecurity in society; or

(b) the use **or threat** is made for the purpose or motive of advancing a religious, ethnic or sectarian cause;

shall be punished with imprisonment of either description for a term which may extend to **fourteen years** or with fine which may extend to fifty million rupees or with both.
Sections 5 & 7

5. Unauthorized access to critical infrastructure information system or data.- Whoever with malicious intent gains unauthorized access to any critical infrastructure information system or data shall be punished with imprisonment upto three years or with fine which may extend to one million rupees or with both.

7. Criminal Interference with critical infrastructure information system or data.- Whoever with malicious intent and without authorization interferes with or damages, or causes to be inferred with or damaged, any critical information system or any part thereof, or critical infrastructure data or any part thereof, shall be punished with imprisonment which may extend to seven years or with fine which may extend to five million rupees or with both.
CYBERTERRORIST?

Angry rants **COULD BE** construed as a threat…

I'M RUNNING AROUND FACEBOOK KILLING ALL THE STUPID PEOPLE PLEASE SHARE ME SO I CAN GET THEM ALL!!

i HAVE HAD ENOUGH OF WATEEN. I'M GOING TO GO TO THEIR HEAD OFFICE AND KILL THEM ALL TILL THEY'RE DEAD!! UGH
Section 16: Offence Against Natural Dignity of a Person

16. Offence against dignity of natural person- (1) Whoever, with malicious intent, knowingly and publicly exhibits, displays, transmits any electronic communication that harms the reputation of a natural person; threatens any sexual acts against a natural person; superimposes a photograph of the face of a natural person over any sexually explicit images; distorts the face of a natural person; or includes a photograph or a video of a natural person in sexually explicit conduct, without the express or implied consent of the person in question, intending that such electronic communication cause that person injury or threatens injury to his or her reputation, his or her existing state of privacy or puts him or her in fear for him or her safety shall be punished with imprisonment for a term which may extend to one year or with fine which may extend to one million rupees or with both.
Provided that it shall not be an offence under this section if the electronic communication is an expression of opinion in good faith not done with malicious intent, is an expression of criticism, satire or political comment or is analogous to any of the Exceptions under section 499 of the Pakistan Penal Code Act, 1908:
Jailed for Memes!

People and outlets that produce such cartoons and memes can be jailed for up to a year or fined up to a million rupees...
Section 16: Spamming

19. Spamming.- (1) Whoever transmits harmful, fraudulent, misleading, illegal or unsolicited intelligence to any person without the express permission of the recipient, or causes any information system to show any such intelligence commits the offence of spamming.
Intelligence is Defined as…

- any speech, sound, data, signal, writing, image or video;
Ever asked your friends to fill in a survey via Facebook or email? Under this law, you can be charged for it being ‘UNSOLICITED INTELLIGENCE’ because you did not get their permission first to send them a message!
Section 18: Cyber Stalking

18. Cyber stalking.- (1) Whoever with intent to coerce, intimidate, or harass any person uses information system, information system network, internet, website, electronic mail or any other similar means of communication to,-

(a) communicate obscene, vulgar, contemptuous, or indecent intelligence;
(b) make any suggestion or proposal of an obscene nature;
(c) threaten any illegal or immoral act;
(d) take or distribute pictures or photographs of any person without his consent or knowledge;
(e) display or distribute information in a manner that substantially increases the risk of harm or violence to any other person commits the offence of cyber stalking.
Took a picture in public that captured someone in the background without their consent – CRIME

Good-bye Facebook, Snapchat and Instagram!

Covered an event, took pictures and shared them to be published – CRIME

Looks like the media’s photography and press coverage days are over…

Sent a picture that did not conform to someone’s view of decency – CRIME
PROCLAMATION.
EDUCATIONAL DECREES
No. 31

POWER TO ISSUE
DIRECTIONS FOR REMOVAL OR BLOCKING
OF ACCESS OF ANY INTELLIGENCE THROUGH
ANY INFORMATION SYSTEM:
The Authority or any officer authorized by it in this behalf may
direct any service provider, to remove any intelligence or block
access to such intelligence, if it considers it necessary in the
interest of the glory of Islam or the integrity, security or defence
of Pakistan or any part thereof, friendly relations with foreign
states, public order, decency or morality, or in relation to
contempt of court, commission of or incitement to an offence.

I solemnly swear that I am up to no good.

BOLO BHI
Advocacy - Policy - Research
ARTICLE 19 & 19A TO BE POLICED BY PTA

Surf Safely

This website is not accessible

The site you are trying to access contains content that is prohibited for viewership from within Pakistan.

THIS WILL NOT ONLY BE THE INTERNET, BUT CONTENT TRANSMITTED THROUGH ANY DEVICE/INFORMATION SYSTEM BASICALLY…
This will be our life after this law is passed in its current form, especially Section 31....
Resources

- Version of the bill and our analysis:
  http://bolobhi.org/whats-brewing-pakistans-proposed-cybercrime-law/

- Online petition asking legislators to make the bill public and seek public input:

- Poster campaign: Writing on the Wall http://bolobhi.org/resources/timelines/writing-on-the-wall/

www.bolobhi.org    www.vimeo.com/bolobhi