GLACY+
Global Action on Cybercrime Extended
Action Globale sur la Cybercriminalité Élargie

Funded by the European Union and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Implemented by the Council of Europe

EU/COE Joint Project on Global Action on Cybercrime:
2016 Octopus Conference
Workshop 2
Legislation on cybercrime and capacity building in the Asia/Pacific region

Do's and Don'ts
Pakistan: A Case Study

Zahid Jamil
Council of Europe Expert

Strasbourg 16 November 2016

KINGDOM OF ABE

- **Sovereign**
- **I can do better**
- **I'm different**
- **I don’t need Experts**

DON'T: Avoid Omnibus Legislation

Let Cybercrime be **CYBERcrime**

NOT = **Crime using Cyber** / **National Security/War**

Limit = Data/Network/Systems Offense

- Kingdom of Abe's Cybercrime law provides for:
  - Terrorism [**decriminalize**, **soft forum**] offences
  - Pornography,
  - Dignity,
  - False Information (opinion, comment, editorial)
  - Stalking (follow/contact/Monitor/watch/**photo** w/o consent)
  - Spamming (show/transmit **any** message w/o consent)
  - CERTs
  - Telecom regulator block websites [against **glory of Islam**]
  - Cyber War (**Prevention** Measures – **Mandate Use**)
  - Privacy/Confidentiality
  - **BUT NOT CYBERCRIME?**
- Fail **dual criminality** test for international cooperation

DO: Be Consistent

- *"unauthorized access" means access to an information system or data* ***which is not available for access by general public****, without authorization or in* ***violation of the terms and conditions of the authorization****;*

- *"****authorization****" means authorization by law or by the person empowered to make such authorization under the law.*

  Provided that where an information system or data is available for ***open access by the general public****, access to or transmission of such information system or data* ***shall be deemed to be authorized*** *for the purposes of this Act;"*

- **Website hacking decriminalized**

DONT: Under-criminalize

- High Mens Rea threshold "**dishonest intention**"
- *"dishonest intention" means* ***intention to cause injury, wrongful gain or wrongful loss or harm*** *to any person or to create hatred or incitement to violence;*
- Requires **proof** of **injury, loss, harm** to a **person** for illegal access, interference, interception- all Cybercrimes

---

- Malicious code: "resulting in the **corruption, destruction, alteration, suppression, theft or loss** of the information system or data"

Don't: Short cuts

Confidentially of information. – Notwithstanding immunity granted under any other law for the time being in force, any person including a service provider while providing services under the terms of lawful contract or otherwise in accordance with the law, or an authorized officer who has **secured access to any material or data containing personal information** about another person, **discloses** such material to any other person, **except** when required **by law**, without the **consent** of the person concerned or in breach of lawful contract with the intent to cause or knowing that he is likely to **cause harm, wrongful loss or gain to any person** or **compromise confidentially** of such material or data shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to one million rupees or with both.

Provided that the **burden of proof** of any defense taken by an accused service provider of an authorized officer that he was acting in good faith, shall be **on such a service provider** or the authorized officer, as the case may be.

DON'T: Reinvent the Wheel
DO: Engage international expertise

- **Use** and **improve** existing **best practice** legislative language

- **Budapest Convention**, Commonwealth, international best practice **model laws** tried & tested

- Legislators without technical expertise may draft ineffective cybercrime laws

DON'T: Be Technology-specific

- Technology-specific language is **restrictive**
- BC is not technology-specific and still relevant
- Technology-specific language becomes **redundant over time**
- **Best Practice: BC, Commonwealth**
- **DO: Define conduct (UK Computer Misuse Act)**

DO: Use Safeguards

- Investigators may issue **production order without warrant**
- Court may allow real-time collection of "**any information**" rather than "**specially-identifiable communications**"
- Court search and seizure warrants **without grounds/safeguards/conditions**
- **Decrypt and provide any data without warrant**
- **Little distinction b/w traffic/subscriber/content powers**
- **No Specific International Cooperation Mechanisms**

EFFECT:

- Countries will be reluctant to **exchange information and cooperate**

Effect of PECA 2016

POLITICIZED - SELF DEFEATING

Joining the BC

- Unlikely that Kingdom of Abe will be able to join BC

International Cooperation

- Unlikely that Kingdom of Abe will be able to gain access to cooperation from BC member states
- Unlikely that other states that were previously cooperating will continue to cooperate on bilateral basis

Legislative Do's and Don'ts

Do:

- Be consistent with best practice (focus on enabling cooperation)
- Engage international expertise
- Use appropriate procedural safeguards

Don't:

- Enact omnibus legislation
- Be technologically specific
- Over-criminalize
- Under-criminalize
- Reinvent the wheel

STORY OF ABE

- **Sovereign**
- **I can do better**
- **I'm different**
- **I don’t need Experts**

Questions

Thank you!

Zahid Jamil, Esq.
Barrister
zahid@jamilandjamil.com