BOLO BHI
Advocacy - Policy - Research

Conceptual Framework for Amendments:

1) Omit sections that are already covered under existing laws; contravene constitutional rights; criminalize what should be civil offences
2) Amend language of sections that are vague and overbroad; add requirement for malicious/malafide intent for establishment of crime to all offences
3) Subject the powers of authorities to checks and balances
4) Build in procedural safeguards and protections to curb misuse and abuse of this law

TO OMIT:

PECB15	Justification	Examples from existing laws, other jurisdictions & conventions
(t) "intelligence"	This definition should be omitted as a) it is too broad; b) it has been directly copy pasted from the PTA Act and intended to empower the Authority with content management powers. All definitions should be brought in line with globally compatible and accepted ones, as they exist in other laws: e.g. other types of data i.e. traffic and content data; information, systems etc should be defined separately.	For definitions, refer to the Budapest Convention See PECB'14 as approved by the Cabinet Division for some of these definitions

(x) "offence"	The current definition needs to be omitted and offence needs to be redefined. Currently, this conflicts with definition (w) minor. The standard definition of a minor as per law is anyone under the age of 18. This unnecessarily creates confusion, exempting those under twelve while making those above liable. Someone who is twelve and a day old or thirteen will be treated differently though he/she could be as unassuming.	See Section 299a of the PPC See Article 10 (b) of the ICCPR
9. Glorification of an offence and hate speech.	This section criminalizes even the 'preparation' of intelligence even if it is not disseminated. How is this to be determined at all? Then, subsection (a) reads 'glorify an offence or person accused or convicted.' This reverses the innocent until proven guilty principle; a crime has not been established. As per this section, to advocate for a person wrongly accused or convicted of a crime would not just be illegal but punishable by five years in prison or ten million rupees or both. Moreover, critiques of judgments – which are commonplace - could also be criminalized, as would be any voices highlighting miscarriage of justice as they could be misconstrued as 'glorifying' an accused or convicted person. Why is the need felt only to introduce such a provision for the electronic and online medium whereas on-ground glorification and praise of confessed and convicted murderers goes unchecked?	153-A of the PPC and 11W of the Anti Terrorism Act, both cover this. See Article 10 (a) of the ICCPR See Principles 1, 2, 6, 7, 8 and 23 of the Johannesburg Principles See OSCE Joint Statement See: ECHR case Jersild v Denmark (and Article 19's note) See GNI report on Extremist Content and the ICT Sector

15. Unauthorised issuance of SIM cards etc.- 16. Tempering etc. of communication equipment	This makes operators criminally liable whereas this is an already regulated sector and policy directives and existing laws apply. There is no need to add these sections in PECB and further threaten telecom operators who have already implemented SIM verification policy of the government by spending millions of dollars. The PTA under the Telecom Act has tremendous powers to penalize telecom operators for non-compliance of any license conditions and giving more powers to the PTA, FIA and other law enforcement agencies to harass telecom operators is incomprehensible and discourages foreign and local investment.	Both offences are already covered under Pakistan Telecommunication (Re-organisation) Act, 1996 - see Section 31 on offences and penalties See Section 47: Exclusion of telecommunication related offences PECB'14 as approved by the Cabinet Division
Sections 18: Natural Dignity of a Person, 19: Offences against the modesty of a natural person and minor 21: Cyber Stalking,	These are not cybercrimes per se - or rather offences that either occur online or through the use of technology, or cannot be curbed under existing laws. Moreover, the PTA cannot act against content on foreign platforms as was submitted before the Lahore High Court. The way technology and jurisdiction works needs to be understood. These sections should be omitted in their entirety; discussed below are the most problematic provisions. Section 18 is already covered under existing laws. Given that, and the fact that a defamation law already exists, there is no need for this section since it deals with reputational damage. The offence described in Section	Section 18 is already covered under Defamation Ordinance 2002 and Defamation (Amendment) Act 2004 and penalized under Section 500 and 501 of the PPC. Section 19 is partly covered under Section 509 of the PPC and can be further amended to make it gender neutral and more specific. For Section 21 see Sections 503, 506 and 507 of the PPC.

	19, which criminalizes the misuse of photographs and information in sexually explicit conduct is not something that happens just online or through the use of technology. Moreover an exemption has been created only for the broadcast media and not others. Previously Section 18 & 19 were compounded together and a proviso existed that protected speech made in good faith or as an act of political expression etc. Most problematic is that the redress mechanism stipulated flows through not court, but the PTA, allowing for misuse not only by complainants but also the Authority, since it has been left up to its discretion what should be removed or blocked based on a complaint. Moreover, PTA does not have the ability to take action against content on foreign platforms and this would be impossible to implement practically. Section 21 sub-sections (a) to (c) contain vague terms such as 'obscene, vulgar, contemptuous, indecent and immoral. These sub-sections should be omitted. The language in (d) needs to be tightened as this could be broadly applied to public events that are covered by the media or political parties, where consent is not explicitly sought before taking pictures are taken or distributed. Similarly, pictures of public figures are carried in articles to supplement them, or memes are created. Harm could be misused and misapplied to settle scores. Therefore a clear balance needs to be struck in this clause so it does	See Lahore High Court's interim order in the 'YouTube case,' BytesforAll vs Federation of Pakistan, and submissions made by PTA, Google and independent experts Read Islamabad High Court's order (a modified version of this initial order) in Bolo Bhi vs Federation, challenging the PTA and government's power to block content online See Indian Supreme Court's judgment striking down 66a of the Indian IT Act See Manila Principles i.e. II Content must not be required to be restricted without an order by a judicial authority See: Hate Crimes in Cyberspace by Danielle Citron, a professor at the University of Maryland's Francis King Carey School of Law. See Chapters 3, 5 and 6 of the UNESCO Report on Fostering Freedom Online: The Role of Intermediaries

	not criminalize commonplace activity – for those ethical guidelines can be developed. Sections 18: Natural Dignity of a Person, 19: Offences against the modesty of a natural person and minor and 21: Cyber Stalking, allow complaints to be made directly to the PTA. Open-ended language can easily be misused by the complainants or the Authority. The interpretation of the clauses is not subjected to a judicial process; no already developed jurisprudence would be relied on. An official of the authority would have absolute discretion. Clause [2] in sections 18, 19 and 21 delegates power to the PTA: the determination of the offence and required action has been left to its discretion. Executive authorities must not play judge, jury and executioner or execute the court's function.	
22. Spamming	The transmission of 'unsolicited intelligence' without the 'express permission of the recipient' has been criminalized as per the language of this clause. It is unclear as to how one should acquire express permission. Definition of spamming also not provided; neither is any threshold specified. Spamming can easily be curtailed through filters in email inboxes for example, number-blocking options in mobile phones, do not call lists etc. Something that is a source of irritation need not	Examples of Spam Acts in other countries: Australia: Spam Act 2003 USA: CAN-SPAM Act of 2003 Singapore: Spam Control Act 2007 Canada: Anti-Spam Legislation 2014

	be criminalized allowing people to be thrown in jail. This should be dealt with through policy guidelines and a regulatory framework, not as a criminal offence. Data protection laws need to be introduced to create parameters so that lists of numbers are not swiftly shared or misused for such purposes. Spamming is not part of criminal law. Canadian and US laws for instance, exclude bulk emails while distinguishing between commercial email and setting different standards for those. Moreover, other countries have Spamming Acts or award civil penalties at most, they don't include a section in a cybercrime law.	Read this on the Canadian Anti-Spam Law See Indian Supreme Court's judgment striking down 66a of the Indian IT Act that allowed people to be arrested for 'annoying' or 'offensive' content.'
23. Spoofing	This is not described adequately. Moreover, this is a form of electronic fraud which is already covered under Section 12, therefore it should be omitted.	See Articles 4: Right not be tried or punished twice of Protocol No.7 to Convention for the Protection of Human Rights and Fundamental Freedoms
29. Retention of traffic data	This requirement runs contrary to protecting the right to privacy. There is also no evidence supporting the idea that retention of data has caused a decrease in terrorist activities: Read this. Research shows that countries like Austria, Belgium, Bulgaria, Germany, Greece, Romania and Sweden, have rejected it. These countries continue	See Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data - Chapter 2 See clause 55 in David Kaye's report

	to tackle serious crime without undermining their citizens' civil liberties through blanket data retention. This clause must be omitted as it is a violation of the right to privacy.	under Anonymity See Necessary & Proportionate Principles - specifically Integrity of Communications & Systems See Manila Principles V (e) about intermediaries and disclosure of identifiable information Philippines Supreme Court struck down this provision from their cybercrime law in 2014. Technology experts argued traffic data was identifiable data and therefore infringed privacy and opened doors to mass surveillance.
34. Power to manage intelligence and issue directions for removal or blocking of access of any intelligence through any information system	This clause gives the government/PTA unfettered powers to block access or remove speech not only on the Internet but transmitted through any device, through its own determination. Not only does this infringe fundamental rights of citizens and curbs media freedom but has huge implications where privacy is concerned. This clause would allow the authority – and in turn the government – to acquire powers to order media houses'	See Lahore High Court's interim order in the 'YouTube case,' BytesforAll vs Federation of Pakistan, and submissions made by PTA, Google and independent experts Read Islamabad High Court's order (a modified version of this initial order) in

	web platforms to remove any material they deem inappropriate. Example: criticism of the government or a view contrary to theirs could be removed on the grounds – according to them – that it is 'anti-state' or against 'national interest.' Such excessive powers are unconstitutional – an executive authority cannot be entrusted with a judicial function i.e. interpreting and applying Article 19. As it is, the government and PTA's blocking powers stand challenged in court and this matter is therefore sub judice. The court must be allowed to reach a conclusion in this case; this section must not be used to try and legitimize blocking powers, influence court proceedings or pre-empt a judgment.	Bolo Bhi vs Federation of Pakistan, challenging the PTA and government's power to block content online See Articles 17, 18 and 19 of the ICCPR See Articles 8, 9, 10 and 18 European Convention on Human Rights See Articles 8, 9, 10 and 18 of the Convention for the Protection of Human Rights and Fundamental Freedoms (as amended by Protocols No.11 & 14) See Chapter 2, specifically Articles 5, 8 and 10 of the American Convention on Human Rights See David Kaye's report III Encryption, anonymity and the rights to freedom of opinion and expression and privacy See Principles 1, 2, 5, 7, 8, 10, 11, 12, 13, 14 and 23 of the Johannesburg Principles

		See Manila Principles See GNI principles on Freedom of Expression and Privacy See Chapters 2, 3 and 5 of the UNESCO Report on Fostering Freedom Online: The Role of Intermediaries Refer to case: Yildirim v.Turkey And commentary by Open Society and Article 19
43. Prevention of electronic crimes	This clause allows the government to issue guidelines from time to time and makes it an offence if they are not complied with. Problems as have appeared in this law could very well appear with the guidelines, which could be issued without thorough technical expertise or knowledge of the medium, placing an unrealistic burden on service providers to do something, which may not be practically implementable or possible to do. This also negates the intermediary liability protection offered to service providers in Section 35. Guidelines to the extent that they break down laws for the benefit of citizens and businesses are another	Refer to Manila Principles I (d) intermediaries should not be required to monitor content proactively

	matter. Around governments play a pro-active role through public messaging to inform citizens about crimes, laws and how they apply, and what they can do (see Canada's anti-spam government website). Similarly in the United States, the Federal Trade Commission issued a Compliance Guide for their Spam Act. The Khyber-Pakhtunkhwa government has done the same with its web portal for the Right to Information Ordinance 2013. These are advisories or easy to understand manuals at best, and that is all the government's guidelines should attempt to do.	

TO AMEND:

PECB15	Justification	Examples from existing laws, other jurisdictions & conventions
(j) "critical infrastructure"	Definition of critical infrastructure should include private businesses as well, not just government infrastructure.	
(q) “identity information”	This needs to be more specific and detailed.	See PECB’14 as approved by the Cabinet Division Refer to definition (l)
(aa) "service provider"	Definition of service provider needs to be amended. (iii) is extremely vague. As per the definition in clause (iv) service providers – traditionally ISPs and telecom operators - has been expanded to now include any place that offers access to the Internet, to the public, i.e., restaurants, malls, hotels, airports, stations and the additional burden of retaining traffic data has been placed on them – and they can be punished for not doing so. This is unrealistic and increases the cost of business.	See definition in Budapest Convention
(dd) “unauthorized access"	dd) Definition of unauthorized access needs to be elaborated upon. In what form would authorization be required is unclear. If someone verbally authorized another to use their laptop, which is a common practice among peers and colleagues, and then to malign the individual the authorizer decided to maintain	See definitions (y) & (z) PECB’14 as approved by the Cabinet Division See definition in Budapest Convention

	authorization was never given and there exists no proof of it, that would become punishable? Proviso protecting against accidental breach or unintentional access and whistleblower protection should be added.	
Section 3: Unauthorized access to information system or data and Section 4: Unauthorized copying or transmission of data Section 5: Unauthorized access to critical infrastructure information system or data Section 6: Unauthorized copying or transmission of critical infrastructure data	These sections should contain a proviso/exception for whistleblower protection. Otherwise an act such as acquiring and disseminating copies of this bill for instance would be criminalized. The state could use this to control information and hold records that should be made public, but would remain classified and illegal to acquire. This will especially impact journalists.	For whistleblower protection see NADRA whistle-blower system , Khyber Pakhtunkhwa's right to information law and the Federal Board of Revenue (FBR) is seeking to do the same through the Finance Act 2015 See Principles 16-18 Johannesburg Principles

10. Cyber terrorism.	The clause reads 'whoever threatens to commit any offence.' This section carries an imprisonment term of fourteen years. While the commission of an offence should be punishable, anything can be construed as a threat. This section also requires a proviso for ethical hacking/white-hat hackers, hobbyists who conduct activities to identify security breaches in systems. It should also protect teenagers from getting implicated as cyber terrorists and jailed for fourteen years, for something they may have done out of boredom – which needs to be reprimanded and dealt with differently.	See Principle 22 Johannesburg Principles See Necessary & Proportionate Principles on Proportionality
Section 11: Electronic Forgery and Section 12: Electronic Fraud	These sections should contain explanations or illustrations due to the technical nature of these offences, to assist the court in establishing the crime. There should also be an assessment process to determine the degree of damage so punishment is awarded proportionately. Some mention should also be made of recourse available to a person to retrieve information/data and be compensated for loss.	See Articles 7 and 8 of the Budapest Convention Read here a paper on Computer-related fraud and Identity Fraud by a Professor from the Faculty of law at the University of Verona
Section 14: Unauthorized use of identity information	Here too, sub-clause (2)(1) enables an application to be made to the Authority (i.e. PTA) and the Authority "may take such measures as deemed appropriate for securing, destroying or preventing transmission of identity information." Too many discretionary powers are	Refer to California Criminal Law: Unauthorized use of Personal Identifying Information

	being awarded and there is the likelihood of invasive techniques being used to do the above.	Read here a paper on Computer-related fraud and Identity Fraud by a Professor from the Faculty of law at the University of Verona
Section 20: Malicious Code	A proviso/exception needs to be created for this clause. What may be deemed as 'malicious codes' or 'viruses' are taught and written as part of academic disciplines. That is how software is developed to combat them. An exception for this should be clearly stipulated or it would create a sense of fear among academics of being potentially charged for a crime, and create hesitation to apply what is learnt in this discipline for legitimate purposes. Moreover, most USBs carry viruses – oftentimes without the knowledge of the owner. Scenarios in which unwittingly a USB transmits a virus should be accounted for. The manner in which this offence would be determined should be specified in clearer terms.	
26: Establishment of investigation agency	The sole responsibility of forensic analysis lies with FIA or the designated investigating agency. The courts would have no technical qualification to analyse the reports and report of investigating agencies would be considered final by the courts. There has to be a neutral and independent forensic agency which provides computer and network forensics analysis in the court.	See Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data - Chapter 2 See Necessary & Proportionate Principles on Integrity of

	Previously, FIA has wrongly prosecuted innocent IT professionals on basis of a wrong IP address provided to them by PTA and safeguards are necessary in order to protect innocents. The investigation authority should not conduct forensics. An independent, statutory body should be established that conducts forensic analysis. This should not be a body such as the PTA that takes directions or policy directives from the government - that defeats its independence.	Communications & Systems & Safeguards against Illegitimate Access and Right to Effective Remedy
Section 27: No warrant, search, seizure or other power not provided for in the Act	The officer should have to go to court and require a warrant for search, seizure and arrest and provide detailed reasoning, in writing, for why it is required.	Section 54-A CrPC (as amended) requires the person being arrested to be informed of the grounds of the arrest. See Section 17 of PECB'14 as approved by the Cabinet Division See Articles 9, 14, 15 & 17 of the ICCPR See Principle 20 and 24 of the Johannesburg Principles

Section 28: Expedited preservation and acquisition of data	This gives an "authorized officer" the unilateral and unchecked power to order the data to be handed over, or be preserved whenever the officer believes it is "reasonably required for the purposes of a criminal investigation" and there is risk the data may be later inaccessible. While the authorized officer is required to notify a court of such requests, the provision does not require the court to examine the legitimacy of the request or impose any particular safeguards for rights. When combined with expansive data retention requirements under Section 29, this article raises serious concerns about unrestrained government access to private communications. This too should be subjected to a court process and not left to the discretion of an officer.	See Section 18 (2) and (3) of PECB'14 as approved by the Cabinet Division See Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data - Chapter 2 See Necessary & Proportionate Principles on Proportionality, Competent Judicial Authority, Public Oversight, Integrity of Communications & Systems See clause 55 in David Kaye's report under Anonymity
30. Warrant for search or seizure	The stakeholder version as approved by the Cabinet Division required investigation officers to provide detailed reasoning, in writing, when applying to obtain warrants. It required the court to depute a Magistrate to accompany the officer – one who had no connection to the special investigation agency in any way – and restrained the court from issuing a warrant for the search and seizure of **'any'** premises, information system etc unless after investigation on the basis of specified contents of the application fell short of yielding	See Section 19: Warrant for Search and Seizure PECB'14 as approved by the Cabinet Division

	results and thereafter required broader access. A penalty was also prescribed for anyone who acted misused powers under this, maintaining a check and balance. Furthermore, citizens were protected against self-incrimination. These are extremely important procedural safeguards and must be reinserted.	
31: Warrant for disclosure of data	In the stakeholder version the corresponding clause pertained specifically to traffic data, and not data in general. The other modification allows the court to order a person in control of the information system or data to 'provide data or access' to the investigating officer. Previously, the clause required the person in control of the information only to 'disclose sufficient traffic data about a specified communication.' Not hand over data or access to such data. That too, the communication a person was required to disclose was for the explicit purpose of 'identify[ing]' the following: *(a) the service providers; and* *(b) the path through which the communication was transmitted.* The list of qualifications of an investigation officer's request for a warrant have been removed as have	See Section 20: Warrant for for disclosure of traffic data PECB'14 as approved by the Cabinet Division

	protection against self-incrimination and misuse of power and need to be put back in.	
Section 32: Powers of an authorized officer	Sub section (g) gives an authorised officer 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 decryption information necessary to decrypt data required for the purpose of investigating any such offence." While the provision provides certain guidance on the way such power should be exercised (acting with proportionality, avoiding disruption, seizing data only as a last resort), the powers vested on the officer are very broad and particularly invasive of the privacy of individual's digital communications. Their potential for misuse is extremely high. This is particularly so as the power provided could be used to demand the disclosure of encryption keys, thereby exposing individuals at the risk of disclosure of private data beyond what may be necessary to conduct an investigation. This will have adverse implications especially on the industry, in terms of data security, and no foreign company would be willing to sign MoUs with a local company if security can be infringed in this manner. This should be removed. Exercise of powers should be subject to clear checks and balances to curtail misuse since this section contains intrusive powers. Miscarriage of justice and	See Section 41 of the ETO on Immunity against disclosure of information relating to security procedure - this conflicts with it See Section 21: Powers of an Investigating Officer and Section 27: Immunity against disclosure of information relating to security procedure in PECB'14 as approved by the Cabinet Division See Necessary & Proportionate Principles on User Notification Refer to David Kaye's report, particularly IV. Enabling restrictions on encryption and anonymity, especially 45

	violation of powers should also be accounted for and penalized.	
Section 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 Act (as it was in the stakeholder version). Data is sensitive information and how it is seized, handled and preserved needs clear and stringent guidelines. The stakeholder version dealt with this in great detail.	See Sections 23: Dealing with seized data & 24: Dealing with seized information systems PECB'14 as approved by the Cabinet Division See Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data - Chapter 2 See Necessary & Proportionate Principles on Integrity of Communications & Systems & Safeguards against Illegitimate Access and Right to Effective Remedy
Section 35: Limitation of liability of service providers -	Service providers should not be required to keep data indefinitely, neither should they be bound by secrecy for unlimited or particularly long periods. The requirement for confidentiality for the first 14 days does not require court's authorisation, and is left to the sole discretion of	See Necessary & Proportionate Principles on User Notification See GNI principles on Freedom of Expression and Privacy

	the authorised officer. Secondly, there is no maximum time limit to the extension of such confidentiality that a court may grant. Procedural safeguards must be added.	See Manila Principles
Section 36: Real-time collection and recording of intelligence	This clause in the stakeholder version pertained to 'Specifically identified electronic information' has been replaced by 'intelligence or data,' which is too broad. Similarly, 'traffic data or content data' has also been replaced with 'intelligence and data.' The current version allows data to be recorded by a service provider 'in coordination with the specialized investigation agency' which absolutely must not be permitted. If at all this needs to be done, the court, service provider and agency should remain independent of each other – be it the collection or provision of information. The stakeholder version outlined certain parameters, which have also been removed and must be reinserted.	See Sections 30: Real-time collection and recording of data PECB'14 as approved by the Cabinet Division See Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data - Chapter 2 See clause 55 in David Kaye's report under Anonymity See Necessary & Proportionate Principles on Proportionality, Competent Judicial Authority, Public Oversight, Integrity of Communications & Systems See Manila Principles V (e) about intermediaries and disclosure of identifiable information

Section 37: International Cooperation	The Act gives the Federal Government unregulated, arbitrary powers to share information with international governments/agencies without any oversight. In sub-section (3) the Act attempts to limit international governments to keep the information confidential or use it subject to some conditions. International governments are neither bound by this Act nor by any such conditions that Pakistan's Government may subject the information to. In the absence of data protection and privacy legislation, it is 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 other foreign companies and governments, to maintain strict checks and balances and avoid violation of privacy.	See Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data - Chapter 3 & 4 See Necessary & Proportionate Principles on Safeguards for International Cooperation See Manila Principles V (e) about intermediaries and disclosure of identifiable information
Section 38: Offences to be compoundable and non-cognizable	Given the excesses committed by investigation agencies in the past, there is little faith that innocents will not land up in jail and be denied bail as they have in various cases – this trend has been noted in FIA cases where bail is deemed as ultimate relief. Currently, Sections 10 and 19 are non-bailable offences. 19 most certainly should not be in this category and given past track record, even 10 should be removed.	See Principle 22 of the Johannesburg Principles

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.	
46. Power to make rules and 47. Removal of difficulties	In the interest of transparency, either as a separate section following this one, or through sub-clauses added to this section, there should be a requirement to make public rules the government develops for a period of at least thirty days, for public input. There is precedent for this in existing law - see ETO. Same should apply for section on removal of difficulty.	See Section 44 of the ETO
48. Amendment of ETO and pending proceedings	Sub-section (2) states proceedings pending under the repealed shall be deemed to have been taken or initiated under this Act. This Act should not apply retrospectively.	
49. Savings of power	This should not be used as another indemnity clause that allows excesses by state institutions; they should be subject to checks and balances.	

TO ADD:

Definitions	There need to be very specific definitions i.e. information system, device, data, traffic data, content data which is currently not the case with the proposed legislation.	For definitions, refer to the Budapest Convention and Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
Protected Data and Information	Since there is no data protection legislation in Pakistan and much of this legislation deals with invasive methods of dealing with information systems and data, the concept of 'protected data/information' needs to be emphasized, as do standards for privacy.	See Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data - Chapter 2 See Articles 17 of the ICCPR See Article 8 of Convention for the Protection of Human Rights and Fundamental Freedoms (as amended by Protocols No.11 & 14) See Article 11 of the American Convention on Human Rights See Necessary & Proportionate Principles on 'protected information,' Integrity of Communications & Systems & Safeguards against

		Illegitimate Access and Right to Effective Remedy See II Secure and private communication in the digital age in David Kaye's report
Rights of the accused	Maximum safeguards and protections need to be built into this law so innocent people are not implicated or framed, and their right to recourse is guaranteed.	See PECB'14 as approved by the Cabinet Division. Refer to Section 42 on Right to anticipatory bail See Articles 9, 10, 14, 15 & 17 of the ICCPR See Articles 2-4 of Protocol No.7 to Convention for the Protection of Human Rights and Fundamental Freedoms See Articles 6, 7, 8 and 13 of Convention for the Protection of Human Rights and Fundamental Freedoms (as amended by Protocols No.11 & 14) See Chapter 2, specifically Articles 5, 8 and 10 of the American Convention on Human Rights

		See Chapter IV: Rule of law and other Matters, specifically Principles 20-22 and 24 of the Johannesburg Principles
Procedural safeguards	In the past, officials of investigation authorities have been involved in threatening and intimidating the accused or, in some instances, held innocent people for crimes they did not commit. Such excesses should be punishable, at the very least with fines and compensation to the accused/victim. Currently, both the PTA and FIA Acts contain indemnity clauses. These should be revisited. Moreover, the above-mentioned authorities or any other agency designated to carry out investigation should be subject to checks and balances in exercise of their powers and judicial and parliamentary scrutiny. Warrants, requirement to qualify them and cordons must be included.	See Section 8 of the FIA Act See Section 33 of the PTA Act See 22, 27, 28, 29, 38, 39, 41, 42, 43, 44, 47 (4) of the PECB'14 as approved by the Cabinet Division