TRA
Lawyers for innovation

Tabular Mapping Of Stakeholders' Responses To Question 11 - TRAI Consultation Paper: Legitimate Exceptions, Exemptions and Lawful Surveillance

---

The following table was prepared after an analysis of all fifty-three (53) responses to question 11 of the Consultation Paper: "*What should be the legitimate exceptions to the data protection requirements imposed on TSPs and other providers in the digital ecosystem and how should these be designed? In particular, what are the checks and balances that need to be considered in the context of lawful surveillance and law enforcement requirements?*"

The table identifies the stances of the stakeholders and their response to the question. It also states the suggestions they have made to the TRAI in view of the question posed. As mentioned earlier, the responses of the stakeholders have been categorised in a manner that corresponds with some of the issues raised in the White Paper, namely, legitimate exceptions for national security and lawful surveillance purposes, exemption of de-identified data from the purview of data protection framework, and checks and balances in context of lawful surveillance and law enforcement requirements.

Sl. No.	Stakeholder	Issues			Recommendations		
		Restricting legitimate exceptions to only critical purposes (such as national security or law enforcement requirements)	**Special provisions for de-identified data**	**Exemptions to TSPs from civil liability claims brought in respect of compliance with exceptions to data protection laws**	**Definition of legitimate exceptions**	**The checks and balances that must be employed in the context of lawful surveillance and law enforcement requirements**	**Other Comments**
1.	Internet and Mobile Association of India (IAMAI)	Exceptions to a data protection law should be restricted to critical purposes such as law enforcement and national security, and should conform to global best practices.	—	Data controllers and processors should be exempted from civil liability for loss of customer data after it is handed over to the authorities in line with the exemptions under the law.	Any exception to the law should satisfy the tests laid out in the Puttaswamy judgment.	A mechanism should be built into the law to ensure uniform applicability of the exceptions.	Data controllers and Internet Service Providers (ISPs) should be permitted to satisfy themselves with the fact that the request is legitimate.

2.	Association Of Competitive Telecom Operators (ACTO)	Exceptions should be statutorily established and limited to circumstances such as national security interests, statutory functions, disclosures required by law or as part of legal proceedings. In addition, there could be several specific exemptions that are particular to the Indian social and economic environment.	__	__	Exceptions should be carefully framed and defined. Exemptions should be based on minimum principles and safeguards of due process such as being based in law, limited to what is strictly necessary for the investigation in question, focus on data of individuals impacted in the crime, be reasoned and subject to review and decision by a court or independent authorities. The persons who can claim the exceptions and the circumstances thereof should be carefully limited.	The scope of bilateral and multilateral agreements should be enhanced for sharing information based on principles of transparency and accountability.	__
3.	The	Exceptions should relate	Anonymised	__	Legitimate exceptions		Prescribing certain

	Associated Chambers of Commerce and Industry of India (ASSOCHAM)	to compelling public interests such as national security and safety, and must manifest in the form of a requirement to comply with legal requests issued in pursuance to the relevant due process requirements.	data should be subject to lower levels of compliance requirement.		must be in conformity with international best practices to prevent regulatory arbitrage.	Checks and balances must be self-regulatory and promoted by the Government encouraging robust cybersecurity norms and practices	minimum standards of encryption would lead to security being incentivised and driven by market forces.
4.	Cellular Operators Association of India (COAI)	—	Publicly available data and anonymised data should continue to be excluded from the purview of data protection requirements.	—	—	—	—
5.	Global System for Mobile	—	—	The Government should provide for limitations of	The framework should be transparent, proportionate,	a) There are already defined legal and licensing methods to deal with law enforcement	The same obligations should be imposed on OTT Communication

	Communications (GSMA)			liability or indemnify telecommunications providers against legal claims brought in respect of compliance with requests and obligations for the retention, disclosure and interception of data.	justified and compatible with human rights principles including obligations under international human rights conventions such as the International Convention on Civil and Political Rights.	agency requests in India, and the process and conditions therein must strictly be complied with. b) There should be a legal process available to service providers to challenge requests which they believe to be outside the scope of the relevant laws. c) Initiatives that increase transparency by publication of statistics related to requests for access to customer data should be encouraged.	Service Providers as are imposed on telecom service providers. The framework should be technology neutral.
6.	Internet Service Providers Association of India (ISPAI)	The rules relating to law enforcement and national security should be applicable universally to all kinds of service providers.	—	—	—	The rules relating to law enforcement and national security should be applicable universally to all kinds of service providers, and no differentiation between entities should be made for this purpose in order to enable authorities to effectively conduct lawful	Security guidelines should include all players and not just limit themselves to Telecom Service Providers (TSPs) alone in order to overcome difficulties such as strong encryption,

						interception of data.	
7.	National Law University Delhi (NLUD)	a) The Puttaswamy judgment recognised that restrictions under the General Data Protection Rules (GDPR) are examples of restrictions to data privacy that may be considered reasonable in India. Convention 108 of the European Union is an international instrument that deals with data protection and also provides for some restrictions. b) NLUD's report lists the permissible grounds of exceptions under the GDPR and Convention 108: National security; Defence; Public security;	__	__	a) Any action that creates an exception, and therefore restricts people's privacy rights in their data must fall within the existing parameters for reasonable restrictions to fundamental rights. b) The conditions under which the International Covenant on Civil and Political Rights (ICCPR)'s Article 17 right can be infringed must be accounted for as well. c) The legislation	__	__

		Other important objectives of general public interest, including important economic or financial interests and scientific research; Protection of judicial independence and judicial proceedings; Prevention, investigation, detection and prosecution of breaches of ethics of regulated professions; Protection of the data subject or the rights and freedoms of others; Enforcement of civil law claims; Prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and prevention of threats to			containing legitimate exception provisions must also contain provisions regarding i) The purpose of processing or categories of processing ii) Categories of personal data iii) Scope of the restrictions introduced iv) Safeguards to prevent abuse or unlawful access or transfer v) Specifications of the controller or categories of controllers		

		public security.			vi) Storage periods and applicable safeguards vii) Risks to the rights and freedoms of the data subjects viii) Right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.		
8.	Span Technologies	Lawful mechanisms can be adopted to intercept terrorist threats rather than subscribing to a blanket surveillance policy.	—	—	—	a) The state needs to strike the delicate balance between safeguarding national security and sovereign interest and ensuring that individual privacy is not	Accountability of all players in the digital arena has to be created for better governance

						imperilled. b) A dedicated, independent, autonomous Authority with a well-defined mandate for data and privacy protection needs to be set up at the national level and should oversee observance of fully secure data integrity practices.	
9.	TRA	__	__	__	__	__	__
10.	The National Association of Software and Services Companies (NASSCOM) - Data Security Council of India (DSCI)	The future data protection law should clearly call out situations of public emergencies or national security with indicative examples for enhanced clarification. Legitimate exception should only be on legal grounds.	__	__	Legitimate exceptions should only be on legal grounds. The law should clearly call out situations of public emergencies or national security with indicative examples for enhanced clarification.	a) Law enforcement agencies should be asking for legitimate and specific data points, and demands for generic data dumps should be avoided. b) The law should have judicial interventions and oversight for surveillance and lawful access to data. c) The legal regime should enhance privacy safeguards based on sensitivity of the data being	The processes to be followed by data processors should be clearly defined in the contracts by the data controller which should not put unreasonable liabilities onto data processors.

						accessed/interpreted d) Since TSP's have multiple layered dependency on several vendors, data controllers should ensure that all connected vendors and sub vendors should adhere to the privacy policy.	
11.	The App Association (ACT)	__	__	__	__	__	Small businesses should be exempt from the rules' requirements in order to ensure that key innovators are not driven out of business by the cost of compliance.
12.	Zeotap India Pvt Ltd	__	De-identified data that reasonably does not allow identification of the individual should not be subject to	__	__	__	The legitimate interests of data controllers should be taken into consideration. An open list of such legitimate interests including research, performance of a contract and marketing could be adopted.

			restrictions.				
13.	Takshashila Institution	__	__	__	The legitimate exceptions to data protection requirements must be narrowly construed, expressly spelt out and be accompanied by adequate procedural safeguards.	If the State is to engage in lawful surveillance in the interest of national security, it should only do so with clearance from a special body comprising members of the Executive and the Judiciary. This special body would have the power to authorise surveillance that is likely to affect data protection. It can also look at whether the data sought to be collected is necessary and that the collection is only for a specified purpose. Further, it can place restrictions on which other agencies of the State and third parties might have access to the collected data.	__
14.	Information Systems Audit and Control Association	The rights of an individual over their personal data may be superseded with a valid, documented justification,	__	__	__	a) A balance must be struck between the rights of the citizens and national safety and security. b) The Supreme Court ruling in	__

	(ISACA)	such as in issues of national emergency or security,				Puttaswamy must be considered in any deliberations regarding the superseding of individual rights in matters of law enforcement and lawful surveillance. c) Other than in matters of national security, the individual must be afforded the right to be informed/made aware of the information that has been shared by TSPs to government/regulatory agencies or any other parties without their express consent.	
15.	International Business Machines Corporation (IBM)	—	—	—	—	—	a) The Government of India should improve the technical competencies of their workforce, to build capacity to understand

							the rapidly evolving nature of technology, to help prioritise resources and to leverage technological innovation to assist in conducting lawful investigations. b) A new policy should not unnecessarily restrict the processing of personal data, and should avoid ex ante restrictions and limitations on the processing of personal data. c) If the Government were to place ex ante limitations on the kind of data that can be processed, expansive grounds for legal processing should be allowed, which go beyond consent and

							include the legitimate interests of the controller.
16.	Make My Trip	The legitimate exceptions should include a) Data shared pursuant to and within limitations of the Users consent b) Disclosures pursuant to any judicial inquiry or audit process c) Storage of data to comply with the applicable laws d) Absolving the data controller from liabilities due to the breach of data privacy by the ultimate service provider or the product seller to whom the data is shared by the	—	—	—	The exceptions themselves may offer some of the checks and balances for enforcement of the regulations.	—

		Controller as a part of the transaction made by the User e) Disclosure required in any litigation initiated by or being defended by the Data Controller or Processer against the Users					
17.	Access Now	There should be no legitimate interest exception to undermine the responsibility to seek user's consent before processing their data. The use or disclosure of user data for cybersecurity purposes without specific protections for user privacy and security should be prohibited as well. Any exception should only permit the	__	__	__	a) Robust and regular transparency and oversight is needed to prevent abuse and overbroad application. This would involve regular audits, and the implementation of transparency provisions to accepted use or disclosures. b) The Privacy Commission should require service provider's to twice annually report to the commission aggregate statistics on all instances when user data is used or disclosed pursuant to	__

		sharing of user data to the extent that Personally Identifiable Information or other personal data is scrubbed and only "whenever reasonably necessary to prevent future cyber security threats or risk of vulnerabilities". This should be done only to the extent that it does not risk user privacy or security, and only in specific, targeted circumstances.				these exceptions. This report should be made public by the Commission, which should also audit each provider's use of these exceptions, including spot checks on specific instances of excepted use or disclosure. c) Telecom Regulatory Authority of India (TRAI), in coordination with the Dept of Telecom should work to ensure the publication of transparency reports from all Indian TSPs on requests from government agencies, detailing their response processes, user notification policies, compliance rates, reasons for compliance or rejection of the requests, which should be a floor requirement and not a ceiling requirement.	
18.	U.S. India	__	Anonymised	__	__	__	a) A strong encryption

	Strategic Partnership Forum (USISPF)		data should be kept out of the scope of the law, and there should be reasonable exemptions for de-identified data.				regime is a must and cannot be overemphasised, and there should be no backdoors in encryption technology. b) Strong encryption provides a competitive market edge, which the government should promote (including the use of strong encryption) to enable Indian companies to compete in privacy-conscious markets. c) Most data controllers comply with legally valid requests for user data in various jurisdictions, and recognise the government's duty to protect national security and public

							safety.
19.	Information Technology Industry Council (ITI)	Technological advancements have rendered using consent as the exclusive basis for data processing an untenable proposition, and other legal grounds for processing must be acknowledged, such as legitimate interests of the data controller, contractual necessity, fulfilment of a legal obligation or the protection of vital or national interests.	__	__	__	__	a) A new policy should not unnecessarily restrict the processing of personal data, and should avoid ex ante restrictions and limitations on the processing of personal data. b) There needs to be a collaborative effort to improve the technical competencies of the workforce, build capacity to understand evolving technology, to help prioritise resources and to leverage technological innovation to assist in conducting lawful investigations.
20.	Sigfox	Legitimate exceptions	__	__	Graded regulations	a) Checks and balances	__

		could consist in the legitimate interests of the data controller, and where applicable, of other stakeholders in the digital ecosystem processing personal and non-personal data. This could include the need to provide the service requested by the data subject, or the need for technical intervention on the network to ensure the quality of service provided to Data subjects.			stating strong principles and providing authorities with the flexibility to develop progressive or tailored decision or guidance based on clear criterion such as data and applications sensitivity, scope of the services and market maturity are appropriate tools to foster economic developments and to allow for ease of innovation.	pertaining to the law enforcement context should focus on the proportionality between the necessary protection of public order and the protection of individual privacy b) There should not be an excessive burden on stakeholders of the digital ecosystem to the extent that it turns them into co-investigators. c) The burden of costs incurred in responding to law enforcement or surveillance requests must be considered.	
21.	Exotel Techcom Pvt. Ltd.	—	—	—	—	—	—
22.	Koan	Legitimate exceptions should be restricted only for critical purposes such as national security or law enforcement and	The Government may gain access to personal	There should be provisions in the law which exempt data controllers from	Exceptions should conform to the three-fold test of legitimate state interests, which is	—	Data controllers and content providers should be permitted to satisfy themselves with the fact that the request is

		should conform to best practices.	information in an anonymised form for carrying out welfare functions. However, such information must be utilised in a non-discrimi natory manner.	liability for loss of customer data after it is handed over to the authorities in line with the legitimate exceptions.	a) There must be a law in existence in conformity with Article 21 b) There should be a legitimate state aim to ensure that the nature and content of the law impose a restriction in conformity with Article 14 c) The means adopted by the legislature should be proportional to the object and needs sought to be fulfilled by the law.		legitimate since they are the custodians of data.
23.	Internet Freedom Foundation (IFF)	—	—	—	Any individualised interception needs to satisfy the three-fold test of	a) Mass surveillance is illegal and unconstitutional. b) Several safeguards need to be adopted such as	—

					a) Legality b) Need and a legitimate state aim c) Proportionality	promoting secure, encrypted communication and notification of the order of interception to the subject of interception.	
24.	Mozilla	Legitimate exceptions must be grounded in the proportionality and necessity principles, and should not take the form of a blanket exception, even for grounds of national security or public order.	—	—	Principles of proportionality and necessity must be accounted for while defining legitimate exceptions. These principles are: a) Legality b) Legitimate aim c) Necessity d) Adequacy e) Proportionality f) Competent judicial authority g) Due process h) User notification i) Transparency j) Public oversight	The following principles need to be adopted in order to establish adequate safeguards and to balance the legitimate aims with the broader good: a) User security: The Government needs to strengthen encryption and not weaken it, in order to prevent the technology from bad actors b) Minimal impact: Government surveillance should minimize impact on user trust and security by collecting only the information that is needed about specific, identifiable	—

					k) Integrity of Communications and Systems l) Safeguards for international cooperation m) Safeguards against illegitimate access	users, and only if other options for obtaining information are not available. c) Accountability: Oversight bodies should be independent of surveilling agencies, with broad mandates, enforcement authority and transparent processes.	
25.	Internet Democracy Project (IDP)	—	—	—	Legitimate exceptions should be made in the form of clear, proportionate and narrowly tailored requests for data sharing by governmental authorities.	a) There needs to be a procedure which creates a paper trail and accountability mechanisms. b) Several arrangements already in place would need to be altered, such as the confidentiality requirements in the IT Rules (Monitoring of Traffic Data), the lack of information about the status and functioning of the Central Monitoring System etc. Further, a body	A degree of accountability for enforcement agencies needs to be established along the lines of the EU Directive 2016/680 on Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal

						independent from the one involved in the said data processing functions should exercise these checks and balances.	Penalties.
26.	Citibank	For the government, the power of exercising legitimate exceptions should be assigned to the Government or its authorised authority on the grounds of interests of public safety required in the interests of the sovereignty and integrity of India, the security of the State, public order or the prevention of incitement of offences. For the data controller, legitimate exceptions should be permitted under the proposed Indian Telecom	__	__	__	There needs to be regulatory reporting and audits, under the proposed technology enabled architecture of personal data for all TSPs and other stakeholders in the digital ecosystem.	__

		regulatory framework only on requirements of any statutory compliance and not otherwise.					
27.	Indian Software Product Industry Round Table (iSPIRT)	__	__	__	Surveillance and law enforcement requirements must be rooted in appropriate laws, which provide a clear framework for such requests to be made, enforced and audited.	a) An immutable record of lawful requests for surveillance must be maintained to ensure that the laws are being followed, and can be submitted for judicial oversight. b) Every service provider should also publish statistics for these requests in the aggregate on a monthly basis.	__
28.	Centre for Internet and Society (CIS)	These exceptions should be on the grounds of national security, public order, disclosure in public interest, prevention, detection, investigation and prosecution of criminal offences, protection of	__	__	Any legitimate exception to the data protection requirements must be clearly defined in law. These exceptions should be guided by the principles of proportionality,	The following principles should be adopted to ensure that surveillance complies with safeguards and protects human rights a) Legality b) Legitimate aim c) Necessity d) Adequacy	__

		the individual or of the rights and freedoms of others.			legality and necessity in a democratic state.	e) Proportionality f) Competent judicial authority g) Due process h) User notification i) Transparency j) Public Oversight k) International Cooperation l) Safeguards against illegitimate access	
29.	US India Business Council (USIBC)	__	__	__	__	Any government request for information should follow certain principles such as a) Requests must follow an established process b) Requests must be narrowly drawn c) Requests must satisfy legal requirements, and should generally include legal process and judicial review (i.e, a subpoena, court order or search warrant)	a) A data protection regime needs to differentiate between residential services (sold to consumers) and non-residential services (sold to large business customers). The expansive data protection regime applicable to residential services should not be extended to non-residential services. b) Providers should be

							responsible for implementing a privacy program and should be able to demonstrate compliance upon request. Any sanctions for violation of the privacy program should not result in a suspension or prohibition of the personal information treatment activities, or lead to the shutting down of the database.
30.	Disney Broadcasting (India) Ltd	__	__	__	__	__	__
31.	BSA	Law enforcement, intelligence and security authorities should have all the tools at their disposal to combat criminal activity,	__	__	A comprehensive framework that reflects the values of both law enforcement, as well as international law,	a) Orders compelling the disclosure of communications content are issued by a neutral judicial authority, based on a finding of probable cause.	__

		terrorism, and other security risks.			individual privacy and free expression is needed.	b) When the government seeks access to cloud-based data, such orders should whenever possible be served directly on the data controller. c) In exceptional circumstances where such orders are served on a data processor (i.e cloud provider), the framework should respect fundamental principles of international comity and the data processor should not be penalised for declining to comply with a disclosure order when doing so would violate the laws of the country in which the data resides.	
32.	IT for Change (ITfC)	__	__	__	Legitimate exceptionsmust be devised with the highest human rights standards in mind, as per global best	Checks and balances must be devised with the highest human rights standards in mind, as per global best practices and explicitly pass the constitutional test. It is important to develop	__

					practices and explicitly pass the constitutional test.	new data institutions that give shape to the state's role of trusteeship for individual and social data. However, this must be done with due constitutional and statutory protections that are effectively and diligently enforced to prevent data-authoritarianism.	
33.	Software Freedom Law Centre (SFLC.in)	Legitimate exceptions should include: a) Section 69(3) of the IT Act allows for a lawful order to intercept, monitor or decrypt some information. b) Service providers should be allowed to retain data that is necessary for the performance of a legal obligation or a legal procedure. However, law	Data that is fully anonymised with no way to link it back to any person should be allowed to be used and shared in any manner by the service provider.	__	Legitimate exceptions should be limited and narrowly defined to avoid abuse.	a) Orders for interception should not extend to decryption of information that is infeasible for the service providers, or to create backdoors in end-to-end encryption systems. b) Data protection requirements should continue to be imposed on partially anonymised data. c) The freedom of press exception should not allow the press to publish sensitive personal information such as	__

		enforcement should not be able to use this provision to force service providers to collect any data that the service provider would not have collected otherwise. c) Data should be allowed to be used for medical research and other research that would result in societal advancements after the data has been anonymised as far as may be feasible. d) Data that is available in the public domain does not need to fall within the scope of data protection requirements. e) The freedom of press should be upheld by				biometric data d) Data subjects should be informed about law enforcement access immediately after access to their data. In cases where such a notice would jeopardize the safety or security of the state, or investigation or prevention of an offence, the data subject should be informed as soon as such a danger has passed.	

		allowing the press to publish information that is in the interests of society.					
34.	European Business Group Federation (EBG)	—	Anonymised data should be kept out of the scope of the data protection law, and a data protection law should incentivise the processing of such data over personal data where appropriate. There should be, at a minimum level,	—	—	—	a) Encryption is a critical tool that the Government must promote to further national security, public safety and provide a competitive market-edge. b) The new law should make a distinction between data controllers and data processors. The data controllers should be responsible for complying with the law, and the data processors should be responsible for taking the necessary technical and organisational

			reasonable exemptions for de-anonymised data.				measures to secure the data they process on behalf of the controller. The controller-processor relationships are governed contractually, and the law should not intervene in these relationships
35.	AT&T Global Network Services India Pvt. Ltd. (AT&T)	Governments can have a legitimate interest in addressing important objectives such as national security, public safety, law enforcement and preventing harm to children.	—	—	The law should clearly establish the circumstances under which public authorities may issue demands for personal information, the forms that such demands must take and the specific authorities that are empowered to make them.	a) Government legal regimes should respond to technological changes through fair, accountable and uniform procedures that govern when and how private companies may be compelled by the government to provide information. b) Companies should be permitted to challenge demands that appear inconsistent with the legal	—

						framework in court.	
36.	Broadband Internet Forum (BIF)	The Government has a duty to protect national security and public safety.	—	—	The law should clearly establish the circumstances under which public authorities may issue demands for personal information and require judicial interventions and oversight for surveillance and lawful access to data.	a) Harmonisation of the interception regime under the Telegraph Act and the Information Technology Act, by bringing both legislations in compliance with the National Privacy Principles. b) Judicial oversight or authorization concerning interception procedures, standardised orders, notification to affected individuals and prevention of overreach of interception orders. c) Companies should be permitted to report publicly on the number of demands that they receive for personal information on a periodic basis, in order to increase transparency and to inform public debate about the relevant laws.	Encryption is a critical tool that the government must promote to strengthen privacy, national security and public safety. Creating an encryption backdoor will significantly weaken any privacy protections and undermine the security of data. Compliance with legally valid government requests for user data is the default position of most data controllers.

						d) The legal regime should enhance privacy safeguards based on sensitivity of the data being accessed/interpreted. e) Privacy standards should be enhanced to i) Achieve better interoperability for cross border data flows with other countries, particularly the EU ii) Improve the chances of fructifying a India-US data sharing agreement in line with UK-US agreement	
37.	Sangeet Sindan	—	—	—	—	a) Law enforcement agencies should work under judicial supervision to ensure lawful and judicious interception of telecom networks or equipment. Law enforcement agencies should be required	—

						to procure an appropriate order from a court of law in order to hack certain systems or equipment. The technologies, techniques and tools of hacking must be commensurate to the gravity of the crime and the quantum of evidence required in the court of law to prove an offence. It would be better to conduct any hacking in supervision of a judicial officer who is capable of only recording the information that is required for such cases. b) The following should be mandated to the TSPs: i) The privacy policy and statement should be made a part of the consumer subscription form and option should be provided as to the types of data which a	

						consumer would like to share ii) Telephone numbers, IP addresses and emails must be kept confidential iii) A data subject must have the right to privacy in relation to clickstream data iv) The privacy policy must specifically state the period of data retention v) The policy must appoint a data officer for addressing queries and complaints vi) They must develop a security system to check the threat of SIM cloning	
38.	Redmorph	__	__	__	__	__	__
39.	Baijayant Jay Panda	__	__	__	The legitimate exceptions should be narrowly defined, and there should be	a) Any person other than a public servant, or an authority duly authorised by the Central Government to	__

					no surveillance except according to rules prescribed under an Act.	order or conduct surveillance or to assist in pending investigation by competent authority shall be barred from initiating, assisting or conducting surveillance. b) The state shall have the power to collect, process, monitor and intercept personal data only in accordance with narrowly defined reasonable restrictions. c) There has to be a time period prescribed for the surveillance period, which should not be carried out indefinitely. d) Reasonable steps must be taken to ensure security of data collected during surveillance and maintaining confidentiality and secrecy thereof. e) No targeted individual profiling can take place and	

						this shall be deemed a violation of privacy. f) There shall be no storage of surveillance which is not relevant, or after a period of one year since the information was collected.	
40.	Apurv Jain	Under the UK Data Protection Act, 1998, the exceptions to fair and lawful data processing are activated only in the cases of crime and taxation purposes - such as the prevention or detection of crime, the capture or prosecution of offenders, and the assessment or collection of tax or duty. In these cases, individual rights can be restricted.	—	—	a) Exemptions are usually granted on a case-to-case basis under the Data Protection Act 1998 in the UK, and the same must be done in India as well, within broad guidelines. b) There should however, be no blanket policy of exemptions, and certain safeguards must be applied to a case-by-case	The safeguards would require a number of conditions to be met a) It must be established that not releasing the information or informing the individual about the release of the information would prejudice the investigation b) It must be established that there is a direct causal link between the information released and the purpose sought to be achieved c) It must be shown that not granting the exemption would directly lead to prejudice d) The tests of necessity and	Data controllers would not have to fulfill their obligations to tell individuals how their data is processed if doing so would prejudice the crime prevention and taxation purposes.

					evaluation.	prejudice must be applied in every disclosure request.	
41.	Reliance Jio Infocomm Limited (RJIL)	Data sharing with designated law enforcement agencies, in compliance with applicable provisions, and data collected for the purpose of national security may be exempted from data protection requirements.	Anonymised data should be granted an exception from data protection requirements.	__	__	__	OTT communications service providers are fully exempted from data protection requirements, and should be brought under regulatory oversight to bring in policy uniformity.
42.	Bharti Airtel Ltd.	__	__	__	__	__	The regulations with respect to national security need to be applied uniformly to all the stakeholders who are operating in the ecosystem of Internet.
43.	Idea Cellular Ltd.	Following are the identifiable circumstances on which legitimate exceptions to TSPs should be based:	__	__	There should be an explicit demarcation and definition of particular information which can be	__	__

		a) Public emergencies or public interest under which such interception is needed to ensure sovereignty and integrity of the country. b) For the purpose of maintaining public law and order and for prevention of incitement of offences. c) Security of the nation and in order to maintain friendly relations with foreign states.			accessed for the specific purpose. The rules and procedures should be clearly established by the concerned authority.		
44.	Mahanagar Telephone Nigam Limited (MTNL)	Legitimate exception can be based on national security as well as prevention, investigation, detection and prosecution of crimes.	—	—	—	—	There should be a centralized technology which has access to the relevant data.

45.	Reliance Communications Ltd. (RCOM)	LEA requirements and usage of anonymized data are the relevant criteria for legitimate exceptions to the data protection requirements imposed on TSPs.	Usage of anonymized data is a relevant criteria for legitimate exceptions to the data protection requirements.	—	—	—	—
46.	Tata Teleservies Ltd. (TTL)	—	—	—	—	There should be a more balanced approach for facilitating TSPs to challenge an LEA request.	There is no need for introduction of additional requirements for the purpose of lawful surveillance right now. It is because there is already a legal framework in place which deals with the rules pertaining to lawful surveillance.
47.	Bharat Sanchar Nigam Ltd. (BSNL)	The legitimate exceptions may be for the purpose of discharging statutory duties, for purposes of	—	—	—	The Indian Evidence Act, IT Act and DOT security guidelines deal with the procedures and conditions under which lawful surveillance and	—

		national security, and the disclosure of any criminal offence and taxation purpose.				law enforcement are required to be met.	
48.	Telenor	The exceptions have been provided under the European Directive General Data Protection Rules (GDPR) and these should equally apply to TSPs as well.	__	__	__	A signed court order should be required by law enforcement to compel access to personal data from a particular business located in a specific region. TSPs should be able to rely on a well laid down process without fear of penalty.	__
49.	Vodafone	Data protection requirements should be applied only in respect of user identifiable information and sensitive personal information.	Meta data or anonymized data should not be subject to any data protection requirements.	__	__	Rule 6 on Disclosure of information, Information Technology (Reasonable Security Practices and Procedures and Sensitive Data and Personal Information) Rules, 2011 permits disclosures if such disclosure has been agreed to between parties, where the disclosure is necessary for compliance of a legal obligation, sharing with	__

						Government agencies mandated under the law to obtain information or by Order under law.	
50.	Federation of Consumer and Service Organizations (FCSO)	—	—	—	—	—	Users expect that their personal information is protected from any abuse.
51.	Consumer Unity and Trust Society (CUTS)	—	—	—	The exceptions provided by the Supreme Court in the recent landmark judgment which established 'right to privacy' as fundamental right should be taken into consideration.	—	—
52.	Consumer Guidance Society (CGS)	The legitimate exceptions should include promotion and preservation of national security, national	—	—	These exceptions need to be clearly defined. Further, the circumstances under which these	a) The authority on whom the responsibility has been put need to be made accountable. b) No surveillance should be	—

		integrity, and investigation of criminal offences, maintenance of public order, peace and tranquility.			exceptions can be availed should also be clearly set out so as to reduce misuse due to excessive discretionary power. The specific needs of the nations should be taken into account while formulating any such exceptions.	allowed without sanction of the court. Further, any such surveillance should be subject to monitoring authority established by the court.	
53.	Consumer Protection Association (CPA)	Following are the grounds for legitimate exceptions: a) Assessment of taxes b) Protection of rights and freedoms of others c) For the purpose of particular individual's personal, family or household matters. d) National security and defense. e) Prevention,	—	—	—	—	—

		investigation, detection and prosecution of criminal offences.					