Dvara Research

Effective Enforcement of a Data Protection Regime

A Model for Risk-Based Supervision Using Responsive Regulatory Tools

Malavika Raghavan, Beni Chugh & Nishanth Kumar[1]

Abstract

This paper presents ideas for a new approach to enforcement of a data protection regime, based on risk-based supervision and the use of a range of responsive enforcement tools that could be deployed *in advance* of a breach to prevent it, or *after* a breach to mitigate the effects. Building on the risk-based approach to supervision, the model proposes a methodology to identify those entities that potentially pose more risk (to individuals and the system) when the personal data they hold is compromised.

Part 2 of this paper proposes a risk-based framework to identify and classify entities based on the risk they pose when the personal data they hold is compromised, using both qualitative and quantitative components. Part 3 sets out an enforcement toolkit for data protection, guided by the paradigm of responsive regulation (that also employs ex ante tools) to prevent and mitigate the effects of a compromise of personal data. This approach is a departure from the post-data breach sanctions that currently dominate data protection regimes worldwide. Part 4 sets out the features of institutional design and inter-sectoral coordination required for effective implementation of such a model approach for risk-based supervision and enforcement of data protection rights.

Dvara Research Working Paper Series No. WP-2018-01
November 2019
Version 2.0

(Version 1.0 released in July 2018)

[1]The authors work with Dvara Research, Chennai, India. We thank those we engaged with during the development of these ideas, in particular Ms. Bindu Ananth, Mr. David Medine, Dr. Katharine Kemp, Justice B.N. Srikrishna, Dr. Nachiket Mor and Ms. Deepti George. We would also like to thank Mr. Sansiddha Pani for research assistance. All errors and omissions remain those of the authors.

Contents

1. Introduction: Design principles for enforcing data protection

The process of considering a comprehensive data protection law for India has begun, as revealed by the broad swathe of ideas under consideration for this new regime in the White Paper of the Committee of Experts on a Data Protection Framework (Committee of Experts on a Data Protection Framework for India, 2017). Any future data protection authority created to enforce a new data protection regime in India would face certain unique challenges. In particular:

- the regulated space is vast, given the ubiquitous collection and use of personal data by service providers in the modern economy;
- contraventions of the regime may not immediately manifest and when they do, may not have a clear monetary or quantifiable harm, and
- the enforcement perimeter is market-wide, so a future data protection authority will necessarily need to interface with other public institutions regulating different sectors of the economy.

To help tackle these challenges, this paper sets out a vision for an integrated system of risk-based supervision and enforcement using a range of regulatory tools. Such a model can ensure that regulation can meet its objectives and have teeth, despite asymmetries of information and capacity that regulators enforcing data protection regulation must constantly reckon with. This vision contemplates the use of risk-based *ex-ante* system to guide supervisory judgment, which is then applied to a range of enforcement tools to minimize the potential for a data breach *before* such a breach occurs or effectively respond *after* a data breach.

Part 2 of this paper proposes a new framework to identify entities that potentially pose more risk (to individuals and the system as a whole) when the personal data they hold is compromised. The framework proposes the use of qualitative supervisory judgment supported by a quantitative classification matrix to focus supervisory attention more effectively across a vast regulatory space. Part 3 sets out an enforcement toolkit for data protection, guided by the paradigm of responsive regulation (that also employs *ex ante* tools to prevent and mitigate the effects of a compromise of personal data). This approach is a departure from the *post*-data breach sanctions that currently dominate data protection regimes worldwide. Part 4 sets out the features of institutional design and intersectoral coordination required for effective implementation of such an approach for risk-based supervision and enforcement of data protection rights.

2. Methodology

This paper proposes a risk-based model of supervision and enforcement of an economy-wide data protection regime. This research objective lends a theoretical character to the paper. The research methodology for developing the theoretical model has relied heavily on three research methods (i) literature review, (ii) extensive secondary research on the workings of Indian and international regulators, and (iii) discussions with experts.

2.1 Literature review

The theoretical underpinnings of the model are deeply influenced by the nature of post-crisis financial regulation. The Subprime Crisis of 2008 revealed the disproportionate systemic risk generated by large, interconnected financial institutions (Restoy, 2017). It also revealed the limitations of the 'too big to fail' approach and justified directing greater regulatory attention toward systemically important entities (Stephen G Cecchetti, 2011). Building on this intuition, the paper proposes a risk-based model that prioritises the regulation of those entities that might be systemically important i.e. the failure of these entities would affect the data ecosystem significantly. Focussing on the systemic importance of entities, resolves two pressing concerns of a new authority (i) where to begin regulating, and (ii) how to allocate precious regulatory capacity. The development of the risk-based classification matrix for data protection entities has benefited immensely from the literature on systemically important entities produced in the financial sector, post crisis. Critical remarks on the theory of risk-based regulation from Prof Julia Black (Baldwin & Black, 2016) and others and the literature from other regulators on conducting data protection impact assessments have also benefited the ideas in the paper. The ideas on responsive regulation have emerged from critically engaging with the seminal work of Ayres and Braithwaite (Ayres & Braithwaite, 1992) and the more recent works of Prof Graham Greenleaf (Greenleaf, Asian Data Privacy Laws: Trade and Human Rights Perspective, 2014) in the context of data protection. This was complemented with secondary research on Indian administrative law and analyses of several Indian regulators as discussed below.

2.2 Secondary research on the workings of Indian and international regulators

The paper has deployed extensive desk research to understand the legal paradigms guiding Indian regulators and the regulatory toolkit legally afforded to them. Some of the Indian regulators analysed for their tool-kits and operating manuals include the Securities Exchange Board of India (SEBI), the Enforcement Directorate (ED) and the Telecom Regulatory Authority of India (TRAI). The scope of the desk research was also expanded to include international data protection regulators to understand how well-established regulators are tackling the issues of enforcement and supervision. The paper has adapted the practices of several international regulators to Indian context. Some of the regulators include the Information Commissioner's Office (ICO, UK), the Federal Trade Commission (FTC, USA) and the Consumer Financial Protection Board (CFPB, USA).

2.3 Discussions with experts

In many ways, the paper strives to break fresh ground in the enforcement of a first omnibus data protection regime. Discussing these relatively new ideas with experts have given us comfort,

confidence and sharp insights to refine the ideas further. Preliminary ideas have benefited immensely from discussions with Mr David Medine[2] and his experience of enforcing privacy at the Federal trade Commission (FTC) of the USA. Dr Katharine Kemp's [3] expertise on the misuse of data for market power has helped us reflect on indicators being used in the risk-based classification matrix and refine the design of the matrix itself. Discussions with these experts have been very enabling, helping us tide over the gap in literature created due to the lack of precedence similar ideas.

[2]David Medine is CGAP's lead on data protection and security. Before joining CGAP, he served as chairman of the U.S. Privacy and Civil Liberties Oversight Board, an attorney fellow for the Securities and Exchange Commission, and a special counsel at the Consumer Financial Protection Bureau. For more, see https://www.cgap.org/about/people/david-medine

[3]Dr Katharine Kemp is a Senior Lecturer at the Faculty of Law, UNSW Sydney. Katharine's research focuses on competition law (particularly misuse of market power), consumer protection and data privacy in financial services regulation. She has published widely in these fields, including "Misuse of Market Power: Rationale and Reform" (Cambridge University Press, 2018), "Competition Law of South Africa" (LexisNexis) with PJ Sutherland, and numerous peer-reviewed journal articles. For more, see https://www.law.unsw.edu.au/staff/katharine-kemp

3. A new framework of risk-based supervision for data protection

A future authority required to enforce an Indian data protection law will be overseeing a very large regulated space. Consider that India has close to 60 million establishments (not counting those engaged in public administration, defence and compulsory social security activities) (Ministry of Statistics and Program Implementation, 2016). A significant proportion of these establishments will likely be collecting, using or storing the personal data of individuals. However, their activities and their use of this personal data will vary widely. Consequently, certain of these entities can be more "risky" to the system and to individuals if the personal data they hold is compromised.

A framework that identifies entities that pose more risk (to individuals and the system as a whole) when the personal data they hold is compromised, can be very useful to reveal the points of vulnerability in the regulatory space. In the broader regulatory context, it has been recognised that a "*risk-based approach to regulation offers systematised decision-making frameworks and procedures that prioritise regulatory activities and deploy supervisory resources - especially inspection and enforcement - based on an assessment of the risks that firms pose to the regulator's objectives*" (OECD, 2008).

Accordingly, we propose a methodology that could act as a "radar" in a risk-based approach to enforcement. Such a risk-based regime would aim to first identify those entities that are likely to have a larger impact if the personal data held by them is breached or misused. This approach borrows from the thinking around data protection impact assessments (EU General Data Protection Regulation, 2018) and separately, in financial regulation around risk-based banking supervision developed following the last economic crisis (Basel Committee on Banking Supervision, 2011).

Conscious of the differing considerations and contexts of financial regulation and data regulation, it is not proposed to duplicate or borrow directly from the thinking of the Basel Committee on Banking Supervision (BCBS). Rather, we are guided by the principles that informed the BCBS' thinking on risk-based supervision to complement the existing thinking on risk-based data protection regulation. This assists us to envision a new approach for regulators to use to identify institutions whose failure (to protect personal data) would have higher impact to individuals and society as a whole, *in advance* of such failure.

Building on principles of risk-based regulation, we propose a model through which a future regulator could seek to identify entities that potentially pose more risk (to individuals and the system as a whole) when the personal data they hold is compromised. The information to make such assessments would be gained through to a two-pronged approach:

- First, through the use of a methodology whereby a future regulatory authority could assign risk scores to classify entities into (i) systemically important data entities, (ii) medium risk data entities and (iii) low risk data entities.
- Second, these risk scores could be analysed together with the results of privacy impact assessments that could be mandated to be undertaken by entities collecting personal data (as briefly described in Part 2.2 below).

Using this information, a future authority could then use an enhanced toolbox that could be deployed *in advance* of a breach or *following* a breach of personal data to mitigate risks to individuals (as further described in Part 3 of this paper).

3.1 Risk-based classification of entities

The methodology proposed that could act as a "radar" for risk-based enforcement is based on two components:

i. a qualitative component accounting for **supervisory judgement**;

ii. a quantitative component using multiple indicator-based measurement to arrive at a **risk-classification matrix**.

In this approach, qualitative supervisory judgment is seen as the primary factor for initiating enforcement actions based on the regulator's assessment of risk posed to the personal data by an entity. The regulator's qualitative judgment could be aided by a quantitative matrix of indicators that approximates the risks posed by entities. The quantitative assessment is designed only to support the regulator's qualitative judgment since no measurement index can perfectly capture the data risks posed by entities.

3.1.1 Supervisory Judgement

Effective data protection enforcement agencies, such as the US' Federal Trade Commission (FTC) and the UK Information Commissioner's Office (ICO) use the information that they receive about data practices to proactively launch enforcement actions. Over the years, these organisations have created robust channels to receive information. The FTC, for instance receives information from within multi-sector institutions, in addition to analysing its self-managed complaint dataset (Federal Trade Commission, 2018) (Mishkin, 2018). These authorities also use the information appropriately to keep pace with new technologies and uses of personal data, to enforce the timeless guarantees of a data protection regime. Their qualitative judgment finetuned by years of observation and analysis is an integral component of effective supervision of the data protection regime. While exercising this supervisory judgment to launch enforcement actions, regulators are required to be guided by certain principles for sound regulation. The UK ICO is guided by principles of (United Kingdom Information Commissioner's Office, 2013):

- **Transparency:** to be open about its approach to enforcement action, the action that it takes and the outcomes it achieves.
- **Accountability:** it will include information on the use of its enforcement powers in its annual report. It will make sure that those who are subject to enforcement action are aware of their rights of appeal.
- **Proportionality:** it will put in place systems to ensure that regulatory action taken is in proportion to the harm or potential harm caused. It will resort to escalated enforcement when it is satisfied that the risk cannot be addressed by negotiation or other less formal means.
- **Consistency:** it will apply its decision-making criteria consistently in the exercise of its regulatory action powers.
- **Targeting:** it will target regulatory action on those areas where it is the most appropriate tool to achieve the objectives of the proposed legislation.

Previously, we have recommended that a future Indian regulator must consider the following factors when determining the enforcement action to be taken against an entity (s 23(4)(d) of a draft Data Protection Bill, (Dvara Research, 2018)):

- the nature and seriousness of the contravention of the provisions of the data protection regime;
- the consequences and impact of such contraventions including (i) benefit or unfair advantage gained by the entity as a result of the contravention; (ii) loss and harm caused, or likely to be caused in future, to individuals as a result of the contravention; (iii) repetitive or continuing nature of the contravention or default prior to the enforcement actions; and (iv) other contraventions committed by the entity.

A future Indian regulator should create a clear, transparent and evidence-based approach to the exercise of its supervisory judgement. We propose that such supervisory judgment should be assess the degree of risk posed by an entity taking into account the **impact** that its failure to protect data adequately would have on individuals and society, rather than the **likelihood** of such a failure. Such an approach can be used as a "radar" tool to identify entities whose failure to protect data may have systemic consequences. This allows for a forward-looking approach where a future regulator to proactively work with entities to put in place measures to (i) minimise the risk of an occurrence of failure, and (ii) to mitigate the consequences for individuals and for other entities connected to them, if such an occurrence does take place. This can supplement the reactive role of deploying post-breach enforcement tools such as penalties.

However, given that India does not have precedence of a comprehensive data protection regime, a future data protection regulator would have no historic information set or observations to benefit from. Conscious of the nascent stage of data regulation in the country, the model proposes to complement supervisory judgement with an objective framework for the assessment of risk.

3.1.2 Risk-based classification matrix

The quantitative component of this methodology consists of a measurement framework designed to identify "systemically important data entities" using a set of objective and measurable indicators. This approach is inspired by the methodology proposed by the Basel Committee on Banking Supervision for assessing systemic importance of Global Systemically Important Banks (G-SIBs) (Basel Committee on Banking Supervision, 2013). This quantitative indicator-based classification matrix will be used to provide a risk score to all entities. As a future regulator gains more information about the market and the entities within it, this matrix should be iterated and fine-tuned.

A purely indicator-based approach maybe prone to moral hazard risk over a longer-term horizon as entities may be incentivised to game the score to avoid closer supervision. Therefore, we reiterate that the indicator-based measurement approach be used to support the supervisory judgment of a future data protection authority, rather than to pre-empt it.

The objective in this model would be for a future data authority to assess the degree of risk posed by an entity by gauging by the **impact** that its failure to protect data adequately would have on individuals and society rather than the likelihood of such an event. This would lead us to ask: if personal data held with a particular entity was assumed to be compromised, what

would be the impact on individuals and society? If the impact is low or medium, the entity would be classified as "low risk" or "medium risk". If it is likely to have a high impact, then the entity in question would be a "systemically important data entity". Under the proposed approach, all entities can receive a risk score at any given point, based on the impact **if** they suffer an occurrence of failure.

The compromise of personal data collected, stored or shared by an entity due to unauthorised use or breach of such data is defined for these purposes as the ***occurrence of failure***.

To measure the systemic implications of the occurrence of failure in entities handling personal data of users, the methodology focuses on two broad criteria- **Connectedness** and **Concentration**. Connectedness is a measure of the number of entities which will get affected due to the occurrence of failure in the defaulting entity. Concentration seeks to assess the number of individuals that will get impacted by the occurrence of failure, given the size of the organisation. Both criteria together measure the scale of effects of occurrence of failure in one entity, on the system and individuals. These criteria have been informed from the literature on assessing systemic importance of banks, but the indicators are selected to reflect the considerations and context of data protection. Methodologically, the matrix divides each of these two criteria into two indicators and each indicator is measured using a set of variables.

Table 1 provides a snapshot of the criteria and indicators that make up this matrix, which are then unpacked and explained in further detail.

Table 1: Indicator-based Measurement for identifying systemically important data entities

Criteria	**Weight**	**Indicator**	**Variable**	**Sub-weight**
Connectedness	50%	**Interconnectedness**	Number of inward connections	10%
			Number of outward connections	10%
			Whether entity is part of larger group structure	10%
			Whether entity has centralised data storage	10%
		Cross-jurisdictional Activity	Transfers with countries without data protection law	10%
Concentration	50%	**Size**	Count of data records with personal data processed/accessed in last year	20%
			Count of attributes of the records processed in last year	20%
			Revenue of firm in the last financial year	5%
		Substitutability	Number of entities performing similar function	5%

Connectedness This criterion is a measure of the connectivity of data entities. The various direct and indirect interlinkages between entities may increase the severity of the impact of any occurrence of failure, as a failure even in one entity may compromise the protection of personal data at entities connected to it. Connectedness is divided into two indicators:

1. **Interconnectedness** is a measure of the degree of connectivity of an entity that shares, processes or stores personal data. A highly connected entity is one that has arrangements with multiple entities either to avail or share personal data of individuals. The variables used to measure interconnectedness are:

    a. **Inward connections:** measured by the number of entities from whom personal data on individuals is collected/accessed;
    b. **Outward connections:** measured by the number of entities to whom personal data on individuals is disclosed;
    c. **Group structure:** indicated by whether the entity is a part of a larger corporate group and if so, measures the number of entities belonging to the same corporate group,
    d. **Centralised storage:** indicated by whether the entity stores data in a centralised system.[4]

2. **Cross-jurisdictional activity** measures the flow of personal data of individuals across international borders. It is measured by a single variable:

    a. **Flow to countries with no data comprehensive protection law:** measured by the number of entities operating in jurisdictions without a comprehensive data protection regime and with whom the entity shares personal data. In the long term, a future data protection authority could have a grading system for levels of data protection across countries. However, as the global adoption of data protection law is still in a nascent state, in the interests of beginning this process, the model suggests this basic indicator.

Concentration This criterion measures the actual size of the individual institution across various dimensions to gauge its capacity to collect, process or store personal data. A high degree of concentration would imply that any occurrence of failure associated with the entity would result in negative impact for a significant proportion of individuals or the society. This criterion also has two components:

3. **Size** is an important measure. The larger the entity, the larger the impact would be of any occurrence of failure. For example, a large entity is likely to be processing the data of a large number of individuals all of whom would be harmed in case of an occurrence of failure. It is measured by the following indicators:

    a. **Count of data records:** measures the number of individuals for whom the entity processed personal data in the last year.
    b. **Count of attributes:** measures the number of attributes of individuals held or processed by the entity in the last year.
    c. **Revenue:** measures the total revenue of the entity in the past one year.

[4]The robustness of decentralised data architectures has also been in question recently. Research suggests there maybe drawbacks in using decentralised data architectures (Narayanan, Toubiana, Barocas, Nissenbaum, & Boneh, 2012). However, from the perspective of impact of occurrence of failure, centralised data architectures still pose significant threat due to the existence of a single point of failure.

4. **Substitutability** measures the relative size of the entity in the market. The systemic importance of an entity is higher if there are relatively fewer entities that provide the same or similar services. Also, as individuals have fewer options to substitute the entity with it is likely that they will gravitate towards these providers, increasing the concentration of data records held with the entity as well. It is measured by a single indicator:

    a. **Substitute Entities:** measured by the number of entities that provide similar services.

The methodology gives an equal weight of 50% to each of the two criteria for risk scores. Connectedness criterion consists of five variables across two indicators. Each variable is given an equal sub-weight of 10%. The concentration criterion is made up of two indicators of size and substitutability, which are assigned a weightage of 45% and 5% respectively. Each variable would be scored from 0 to 1 by normalising the values of the variables. The total risk score for an entity would be calculated based on the weights and the scores for each variable.

It should be noted that the values for most of these variables will not be readily available to a new regulatory authority. Therefore, there is a need to set up appropriate mechanisms through which entities could report data to the authority for evaluation. In the first year, entities' reporting of these minimal variables may be patchy and consequently we propose a set of proxy variables that could potentially be used to begin creating this matrix for the market in the initial period or "Year 0" at Appendix A (*Framework for Indicator Based Measurement in Year 0*).

It should be noted that distinguishing between systemically important entities, medium risk entities and low risk entities using the scores would involve additional supervisory judgement. Hence, it is proposed that the supervisory authority should evaluate the scores obtained using this methodology and subsequently set the threshold for systemic importance. A purely indicator-based approach to classifying entities may not be adequate, and a future data protection authority must ultimately use all the knowledge and tools available to it for better enforcement. This methodology will have to be revised periodically as the regulator's understanding of the market evolves. This risk-based classification of entities also impacts the choice of enforcement actions of the regulator, discussed in Part 3.

3.2 Results of privacy impact assessments

A privacy impact assessment (PIA) is a systematic assessment conducted within an organisation to identify the impact that a project might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact (Office of the Australian Information Commissioner, 2014)

PIAs are integral tools for risk-based supervision of entities handling users' personal data. The EU GDPR mandates PIAs where a processing activity is likely to result in '*a high risk to the rights and freedoms of natural persons*' (Art.35(1), (EU General Data Protection Regulation, 2018)). Though in its current form, the EU mandated PIA does not list the specific indicators that entities must report on some EU member states have offered guidance on the features to be included in PIAs. For instance, the UK ICO recommends (UK Information Commissioner's Office, 2018) :

- description of the nature, scope, context and purpose of processing;

- compliance measures in alignment with the requirement of the proposed data protection law, including the necessity and proportionality of processing;
- identification and assessment of risks to individuals due to processing of their personal data;
- identify measures that can be deployed to reduce or minimise these risks, and
- adapt operations to integrate these measures identified (in the step above).

Obtaining PIAs from all regulated entities dealing with personal information would ideally support the risk assessment described in Part 2.1 of this paper. This would create more information for accurate analysis for both entities holding data and their regulator. However, cognizant of the varying capacity and sizes of entities in the Indian market, a staged requirement for PIAs could be included during the initial years of future data protection regime. To reduce the burden of compliance, provisions may be considered such as allowing entities with less than 500 employees and having an annual turnover of less than Rs 1 crore (or other suitable threshold) to jointly appoint a service provider to conduct PIAs. A future data protection authority would take into account the findings of the PIA when classifying the entity under the risk-based assessment framework discussed in the previous section.

4. A 'Responsive Regulation' toolkit for enforcement

This section proposes a hierarchy of enforcement tools to promote compliance with a future regime in letter and spirit, as well as allow well-targeted punitive actions for violations of a future law. These tools could be complementary to the risk-based approach to supervision which could provide the regulator some tools to calibrate their use of powers to gather information and take action to prevent contraventions of a data protection regime. Such contraventions may not be easy to discover for a new regulator, especially as manifestation of harm from poor data practices can be delayed or non-quantifiable. A future regulator could benefit from using a combination of soft and hard enforcement tools to encourage bilateral communication about data practices between a new regulator and the entities it regulates.

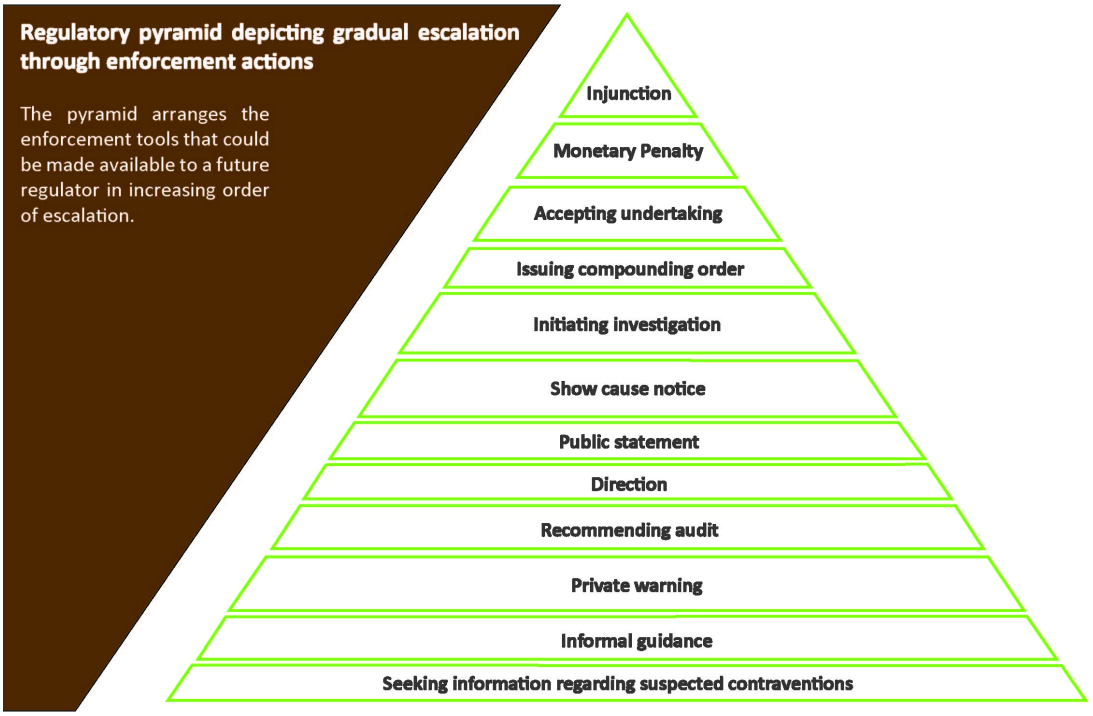
This approach is based on **responsive regulation**, a well-developed academic theory and a widely accepted regulatory framework. It is a dynamic, context-sensitive framework that incorporates multiple kinds of enforcement actions (Ayres & Braithwaite, 1992). The crux of responsive regulation is a hierarchy of multiple kinds of enforcement actions (Greenleaf, Asian Data Privacy Laws: Trade and Human Rights Perspective, 2014) through which a future regulator can escalate. To begin with, the regulatory posture is collaborative. Subsequent contraventions are addressed through gradual regulatory escalation. The magnitude of escalation and the punitive effect of the regulatory response corresponds to the nature of default. The underlying tenet of the model is that a credible threat of an ultimate, serious and costly regulatory imposition will encourage regulated entities to comply earlier with the softer, cheaper regulations such as disclosure and reporting. Compliance is incentivised by the threat of expensive and prohibitive regulatory sanctions (Braithwaite, 2010).

This hierarchy of instruments should not be confused for an inability to use the more punitive regulatory sanctions. The "*timeliness of an intervention to prevent harm trumps low interventionist dialogue*" (Ivec & Braithwaite, 2015). The use of any of the regulatory responses is not excluded from the regulatory toolkit.

4.1 A pyramid of sanctions for a future Indian regulator

Figure 1 (below) sets out a proposed pyramid of sanctions through which a future Indian data protection authority could escalate.

FIGURE 1: Regulatory pyramid depicting gradual escalation through enforcement actions



The pyramid above arranges the enforcement tools that could be made available to a future regulator in increasing order of escalation[5]. A short explanation of these tools is given below.

i. **Seeking information regarding suspected contraventions:** A notice requiring an entity to provide to a future data protection authority such information as specified for assessing whether the proposed regime or related laws have been complied with. See for instance the information notice as used in the UK Data Protection Act 2018. (Information Commissioner's Office, UK, 2018).

ii. **Issuance of informal guidance:** A response from the regulator to a clarification sought by regulated entity. This could be published on a future data protection authority website for the benefit of other relevant entities. Similar tools are used by for instance by Securities

[5]Other regulators in India (like SEBI) and data protection regulators internationally (like the FTC) deploy the responsive regulation framework to achieve regulatory objectives. Through the SEBI (SRO) Regulations 2004, SEBI has allowed for creation of and regulation through self-regulatory organisations. SEBI also offers informal guidance to companies directly and issues direct orders while retaining powers for more punitive regulatory measures' like investigating and penalising defaulting companies (Securities and Exchange Board of India Act of 1992 (as amended by the Finance Act in 2017)). The regulatory stance of the US Federal Trade Commission (FTC) closely resembles the increasing escalation illustrated in the regulatory pyramid. The FTC begins with the assumption of willingness of the regulated entity to comply with the law. Resolution for the first offence is often worked out through negotiations between the FTC and the defaulting company. The complaint and consent decree are triggered simultaneously and filed in federal court and subsequent offences can attract regulatory escalation, monetary penalties sometimes up to of USD 40,000 per individual violation that can be multiplied by the number of users and can be levied on a daily basis for continuing violations (McGeveran, 2016).

and Exchange Board of India (Informal Guidance) Scheme 2003 (Securities and Exchange Board of India, 2018).

iii. **Issuance of a private warning:** A warning letter to advise an entity that certain actions are in contravention with the data protection regime. These are not accusations of wrongdoing and are meant to help recipients review their practices to ensure that they comply with the proposed data protection regime. Similar enforcement actions have also been recommended in the Draft Indian Financial Code, 2013 (Financial Sector Legislative Reforms Commission, 2018).

iv. **Recommending an audit:** An assessment, made with the agreement of the organisation in question, as to whether the organisation's processing of personal data complies with proposed the regime. See for instance the assessment notices as used in the UK Data Protection Act 2018 (UK Information Commissioner's Office, 2018).

v. **Issuance of a direction:** A formal notice/order requiring an entity to take the action specified in the notice, to bring about compliance with proposed the data protection regime. The Telecom Regulatory Authority of India is an existing authority that uses this tool (Telecom Regulatory Authority of India, 2018).

vi. **Issuance of a public statement:** A public announcement, through a future data protection authority website and media, of a contravention of the proposed regime, by an entity who is identified as the wrongdoer, or of a general practice that is of critical public interest. A similar recommendation is also made in the Draft Indian Financial Code, 2013 (Financial Sector Legislative Reforms Commission, 2018).

vii. **Issuance of a show cause notice:** A notice presented to an entity in respect of which a future data protection authority proposes to commence an investigation, before commencing the investigation. Where the concerned entity is under the regulatory purview of an existing sectoral regulator, a future data protection authority could inform the relevant sectoral regulator of the show cause notice of proceedings on commencement of the investigation. India's Enforcement Directorate uses this tool for instance when enforcing the Foreign Exchange Management Act, 1999 (Directorate of Enforcement, Ministry of Finance, 2018).

viii. **Initiation of investigation:** Where a future data protection authority has information or reasonable grounds to suspect that an entity is in contravention of the proposed data protection regime and the contravention is of sufficient public interest to warrant the resource commitment, it may initiate an investigation by appointing one or more investigators to investigate the suspected contravention and record such appointment. See for instance the investigation process followed by the Federal Trade Corporation (Federal Trade Commission, 2018).

ix. **Compounding orders:** A future regulator could compound offences under the proposed data protection regime after the initial investigation where violations are clear, and the concerned entity has consented. Compounding orders could be supported by undertakings (as described below). Similar compounding powers are available to the Indian Enforcement Directorate under the Foreign Exchange Management Act, 1999 (Reserve Bank of India, 2018).

x. **Accepting the undertaking from the compounding order:** A future authority may seek a formal undertaking from an entity, committing them to a course of action or otherwise achieving compliance with the proposed regime. For instance, the compounding

orders of the Directorate of Enforcement are accompanied by undertakings (Reserve Bank of India, 2018).

xi. **Imposition of monetary penalty:** A monetary penalty could be imposed on an entity for the contravention of the proposed regime. In determining the amount of the monetary penalty, the regulator could consider the degree of culpability, any history of similar conduct or contraventions, ability to pay, effect on ability to continue to do business, and such other matters as justice may require. Administrative monetary penalty is a widely-used regulatory enforcement tool across regulators and jurisdictions (Rolfe, 1997).

xii. **Inter-sectoral enforcement actions:** A recommendation could be made by the authority to relevant public authorities and sectoral regulators to take such steps as they may be empowered to take with respect to any entity, including but not limited to temporary suspension of relevant licences or activities. Similar provisions for inter-sectoral referrals exist in India's Competition Act 2000 (Competition Commission of India, Government of India, 2018).

xiii. **Injunction:** A future regulator may seek injunctive relief from a relevant quasi-judicial authority to prevent the continued use of an unlawful data practice. Injunctions are used in the enforcement of the Patents (Amendment) Act 2005 (Ministry of Commerce & Industry, Government of India, 2018).

xiv. **Monitoring compliance:** Monitoring compliance with the enforcement actions issued, orders of the quasi-judicial authority, and other relevant orders.

The tools at the bottom of the pyramid (such as seeking clarification or issuing informal guidance) encourage voluntary corrective action by the non-compliant entity. The failure of the defaulting party to respond to these measures would result in regulatory escalation, such as the imposition of monetary penalties or referrals to sectoral regulators for temporary suspension of activities.

4.2 Use of enforcement tools

This enforcement model includes tools that can be used *before* a breach occurs. They equip a future data protection authority to look beyond post-breach sanctions, which can often be too little too late for those whose personal data is compromised (Raghavan, 2018). This however means the regulator must use such tools wisely, proportionately and impartially. It must look to a wide number of sources for information (including the supervisory methodology noted above) prior to deploying these tools.

Principles to constrain supervisory judgment appropriately have been discussed in Part 2.1.1 above (in supervisory judgment). To maintain consistency and fairness however, enforcement actions should be agnostic to the nature of institution and due investigations must precede punitive enforcement decisions. Investigations should be initiated by presenting timely and

detailed show cause notice[6] to the relevant entity. A future regulator should disclose in advance, the rules, data and informational inputs that will be used to make enforcement decisions, and enforcement actions should also be disclosed in a timely and readily accessible manner. (OECD, 2013).

Consumer complaints data, media reports and breach notifications

When using these tools, a future regulator should seek information on suspected contraventions based on a variety of available information. Information obtained based on the use of the risk-based supervision approach (described in Part 2) would be immensely useful to calibrate the regulator's assessment of whether any enforcement tools need to be deployed. Other sources of information could include media reports of misuse of data or other disclosures made by entities, but also information received through direct complaints from whistle-blowers. An important source of information to guide the use of tools to seek information could also be consumer complaints data. Supervision and enforcement must ultimately be in line with the broader mandate to uphold consumers' rights under a new regime and create redress for grievances. It is well established that effective redress increases consumer confidence and encourages them to avail of the system more frequently (Task Force on Financial Redress Agency, 2016).

It is proposed that a future regulator should filter and record all genuine complaints and enquiries in an open central complaint database. This database could be used to monitor progress on complaint resolution and, also as an analytical tool for researching vulnerabilities in the system. The database should be suitably anonymised and be compliant with the provisions of data protection regime. We also propose creating separate mechanisms for receiving complaints from whistle-blowers to protect their identity.

As a matter of good governance, we propose that a future regulator should provide regular updates to complainants on the progress of their complaint through a communication channel of their preference. Ultimately, the redress mechanism should be accessible, simple to use and should not prove to be burdensome for the consumer, offering them multiple channels to register complaints (such as, toll-free calling lines, central online portal, email, letter, fax and even in person) which will also build up the regulators' visibility on firms' behaviour.

In addition to a central complaint database, data on breach notifications (if mandated by a future regime) should be used to guide the use of post-breach enforcement tools.

Such an approach would allow a future data protection authority to act proactively and uphold the guarantees and enforce obligations under a data protection regime, on an ongoing basis.

[6] Following the insights from The Indian Financial Code, (Financial Sector Legislative Reforms Commission, 2018) a show cause notice issued by a future data protection authority must:
(a) be in writing;
(b) state the action which a future data protection authority proposes to take;
(c) give reasons for requiring the proposed action;
(d) describe the effect of the proposed action;
(e) attach the material that supports the show cause notice; and
(f) provide the recipient a reasonable period to respond, which must not be less than twenty-one days.

5. Institutional apparatus and inter-sectoral co-ordination

Organisational structure is recognised to be a crucial determinant of regulator's performance, including at the level of employees (Carrigan & Poole, 2015). It is also recognised that aspects affecting the design of regulatory policy include the complementary instruments operating in the same space, especially other governmental rule-making bodies which can influence the form, function and scope of regulatory policy (Sappington, 1993).

Any re-imagining of data protection enforcement must therefore consider the basic institutional apparatus required for effective application of the principles described in Part 2 and 3 of this paper. It would also be essential for such an institution to interface and coordinate with a wide range of ministries, regulatory bodies, self-regulatory organisations or industry bodies dealing with personal data. In this section we discuss the structure of governing body that will assist a future regulator to coordinate its various activities and interact with other relevant institutions.

5.1 Institutional design

The model of pro-active data protection enforcement envisioned in this paper would require three attributes for successful implementation from a future data protection authority.

- **Independence:** The independence of a future authority would be core to its credibility and effectiveness. It must be designed in a way that allows it to be receptive to changes in industry, but guard against capture or pitfalls such as ties to incumbents who may delay introduction of services or technologies.
- **Accountability:** A future authority with access to a wide range of enforcement tools must also have robust accountability mechanisms in place to ensure these tools are used fairly and consistently.
- **Effectiveness:** Reflexivity will be required by a future authority so that there is a feedback loop that allows an assessment of whether the regulator's performance and enforcement actions are effectively leading to the fulfilment of the overall regulatory objectives.

5.1.1 Commissioner accountable to a Management Board

A structure that fixes responsibility on a Chief Data Protection Commissioner who reports to a management board would help ensure that these qualities are reflected within a future statutory data protection authority. While a Chief Data Protection commissioner could be in-charge of the regulatory decision making, the management board should be primarily responsible for oversight, scrutiny and guidance on the operations of the regulator (OECD, 2013).

Collegial bodies are generally seen as more independent (as it is less likely that all members would be influenced by the same actors, whether in the government or the private sector), with a greater sense of legitimacy in decision-making, and transparency as the senior leadership has a natural internal accountability lever in the form of the board (ITU-infoDev, 2017). Collegiality

ingrained in management boards offers resistance to regulatory capture and diversity in expertise. (Meloni, 2010). Similar design choices are also reflected in structures of data regulators in other jurisdictions[7].

The composition of the management board must ensure a good mix of independent and government-appointed members. The conduct of members must be laid out, with clearly identified requirements for accountability, including strict procedural requirements, reporting mechanisms, public consultation, and substantive judicial review (ITU-infoDev, 2017). All independent members must also disclose any conflicts of interests and must endeavour to preserve their independence. (Schedule IV Companies Act 2013 could provide further guidance on conduct of independent members). In carrying out its functions, a management board should be guided by clearly identified terms of reference. The UK's ICO for instance has terms of reference that set out mandate and objectives of the management board together with responsibilities, composition, quorum, information requirements, and evaluation of the board and members (UK Information Commissioner's Office, 2017).

Periodic reports from a Chief Data Protection Commissioner to the management board and the public will encourage accountability, improve transparency and confidence in the functioning of a future regulator. A future Chief Data Protection Commissioner could publish, suitably anonymised, monthly reports on the nature, volume and geographic concentration of complaints received in the public domain. This will strengthen the credibility of the regulator and help in detecting early signs of emerging vulnerabilities. A future Chief Data Protection Commissioner should also annually report on enforcement actions undertaken and complaints acted upon, both to the Parliament and in the public domain. Reporting on enforcement actions, consistently in the same format will create a robust framework for ensuring accountability of the future authority. It will ensure that the wide powers afforded through the responsive regulatory toolkit are exercised with great restraint and transparency. Moreover, by exposing itself to the scrutiny of the Parliament and the public, the future authority will elicit trust from market participants and consumers alike. A future Chief Data Protection Commissioner must also report on matters of administration of the future authority including annual plans, budgets, audits and risk assessments to a management board. In addition to supporting the principles of independence, accountability and transparency identified above, these public reports could also encourage academic research in this field.

5.1.2 Complementing institutional apparatus

Some complementary institutional functions required for a future central regulator in discharging its functions are set out in this section.

Regional offices
A future nationwide regulator must contemplate a regional presence, given the complexity and

[7]The work and analysis for this Chapter has benefitted from several national and international regulatory models, particularly:

- The UK Information Commissioner's Office (ICO);
- The Directorate of Enforcement, Ministry of Finance, Government of India;
- The US Federal Trade Commission (FTC);
- The US Consumer Financial Protection Bureau (CFPB), and
- The Report of the Task Force on the Financial Redress Agency (FRA), Ministry of Finance, Government of India.

vastness of the country. This has been recognised by other enforcement agencies in the country. For example, the Directorate of Enforcement which is the specialized financial investigation agency under the Department of Revenue of the Ministry of Finance has five regional offices with zonal and sub-zonal offices in smaller cities (Directorate of Enforcement, Ministry of Finance, 2018). The regional offices could provide an efficient means to undertake supervision and redress activities, engaging more closely with consumers, in regional languages and generate greater awareness among users.

Adjudicating authority
Given the range of enforcement tools, it is important to have a well-structured independent quasi-judicial forum for the regulator to adjudicate on violations of a data protection regime. Members should be a mix of experienced judicial and technical members, with relevant expertise in technology, data science and regulation. Regional benches should exist to improve accessibility, and a clear and effective appeals mechanism should also be clearly established

Legal expertise
A legal team looking across all functions of a future regulator would be essential for (i) drafting regulations and policies for administering future data protection regime (ii) undertaking in-depth legal analysis on new and emerging questions of the law and (iii) working with other sectoral regulators and handle the legal affairs of the regulator (including during investigations and adjudications). This will enable a future regulator to develop a stand on novel and contentious issues.

Research and analysis capacity
A future regulator must have a mechanism to learn from its own information and conduct research. In-house capacity for conducting high quality research (including on the databases maintained by a regulator like a complaints database) could generate policy insights and reveal vulnerabilities in the system, enabling a regulator to address them before they manifest in harms. An analysis of information on breaches or misuse of data could inform the supervision and enforcement activities. The insights generated through internal research will be necessary to assess and finetune the methodology presented in Part 2.

Communications and community outreach
This capability would be required to generate awareness about users' rights, guarantees and protections under a new regime. This is important for both firms and consumers. It is particularly relevant in the Indian context given that awareness about data protection remains low in the country and individuals do not fully understand the risks associated with sharing their personal data with other entities (Dvara, Dalberg & CGAP, 2017).

A **secretariat** function for a future regulator will be needed to undertake administrative aspects of its activities including, financial planning, management, human resources, IT support, office supplies and other support functions.

5.1.3 Intersectoral Coordination

As noted above, a future data protection authority will have a wide regulatory perimeter and need to interface with other regulatory institutions and government agencies operating in different sectors. The use of Memoranda of Understanding between regulators has been recognised as one tool to create pathways for inter-sectoral collaboration on an on-going basis. This approach has been recommended by the Task Force on the Financial Redress Agency, which seeks to

create a new agency to improve consumer protection and redress in India (Task Force on Financial Redress Agency, 2016). The UK's ICO has also successfully entered in a number of MoUs to encourage coordination with other bodies (nationally and internationally) (UK Information Commissioner's Office, 2018).

As a new organisation, the onus will be on a future data protection authority to act to create links with existing bodies in complementary areas of regulation. To begin the process, the regulator's staff must scan the institutional landscape to identify other public authorities, government departments and self-regulatory organisations which are of relevance to its mandate and objectives. This must be an annual exercise, to take account of new regulators that may develop in the country - especially in sensitive and related sectors such as health, telecommunications, finance and home affairs. This approach will allow a future data protection authority to prioritise the relationships it needs to create with regulators based on the level of overlap.

6. Conclusion

This paper has attempted to draw on emerging lessons on risk-based regulation, to create a novel approach for consideration when seeking more effective enforcement of data protection regimes. This attempt has been made given that the traditional approach of post-breach sanctions are proving to have limited use for users and regulators dealing with the effects of improper data use. A more proactive *ex-ante* approach could help focus regulatory capacity on the most serious risks to protection of personal data (Baldwin & Black, 2016). Such a model will require a motivated and well-resourced regulator that will need to be both agile and transparent in its functioning. However, the need to explore new ideas for the regulation and enforcement of data protection regimes appear inevitable in the face of the advances in data use and analytics in the modern, data-driven economy.

References and Appendices:

Appendix A: Framework for Indicator-based Measurement in Year-0

It is recommended that a reporting framework be designed for a future data protection authority to obtain the data it needs inform the risk-based classification suggested in this paper. Creating a reporting framework typically needs time and some iterations before entities can collect and provide the data in the desired format to a future data protection authority. Considering this limitation, the framework offers a special provision for Year 0. Pending the reporting of the required data, the variables of the framework are replaced by proxy variables which may provide an approximation of the relevant indicators. The values for these proxy variables may be obtained from data that is already reported by entities to various public authorities.

It is important to bear in mind that this framework is designed to be transitionary, to overcome the lack of information that may become a barrier for implementation of the classification framework in its early years. By design, this framework is **only an approximation based on available data** and may not truly reflect the impact of an *occurrence of failure*. These proxy variables should be used only for the early year of any DPA's operations, during which time a framework should be established for all entities to report the required data. Once relevant data is available for a significant number of entities, the regulatory authority should stop utilising these proxy variables for classification purposes. The proxy data points for each of the variables are discussed below.

1. **Number of inward connections:** To approximate the number of inward connections, fixed list of activities can be drawn up, comprising activities which are highly likely to rely on numerous inward/outward connections. For example, an entity which provides data processing services is by nature likely to have high number of connections. Similarly, an internet service provider is also likely to have a very large number of inward and outward connections through which personal data flows between various other entities. The creation of this list can be informed by the codes available in the National Industrial Classification (NIC) of 2008.

2. **Number of outward connections:** The list developed for gauging the number of inward connections can be used.

3. **Whether entity is part of larger group structure:** If the entity has one or more subsidiary companies or is controlled by a holding company as per filings with the Indian Ministry of Corporate Affairs, it should be considered as part of a large group structure.

4. **Whether entity has centralised data storage:** As there is no credible way of estimating this from available information, in the interim all entities should be given a score of 0 for this variable.

5. **Transfers with countries without data protection law:** For this variable as well, a score of 0 should be assigned to all entities until reported data is available for the same.

6. **Count of data records with personal data processed:** This indicator could use that number of transactions reported as part of GST returns, as a proxy variable.

7. **Count of attributes of records processed:** For this variable too, all entities should be assigned a 0 score in the interim.

8. **Revenue of the firm:** This data may be obtained from data reported to the Ministry of Corporate Affairs or from GST returns filed by the entity.

9. **Number of entities performing similar function:** The number of establishments having the same NIC Code should be used as a proxy for this variable.

In the first year, based on the values of the above proxy variables, each entity should be assigned a score of 0, 0.5 or 1. The basis for this scoring method is outlined in the table below.

TABLE 2: Proxy variables and scoring for Year-0

Variable	**Proxy variables for Year 0**	**Year 0 Score Range**	**Basis for scoring**
Number of inward connections	Type of firm (with high in-degrees)	No - 0 / Yes - 1	Based on List of NIC Codes which are likely to have high number of connections to other entities
Number of outward connections	Type of firm (with high out-degrees)	No - 0 / Yes - 1	Based on List of NIC Codes which are likely to have high number of connections to other entities
Whether entity is part of larger group structure	Whether entity is part of larger group structure	No - 0 / Yes - 1	If the entity has one or more subsidiary companies, or is controlled by a holding company, based on filings with the Ministry of Corporate Affairs.
Whether entity has centralised data storage	N/A	Cannot estimate - 0	
Transfers with countries without data protection law	N/A	Cannot estimate - 0	
Count of data records with personal data processed/accessed in last year	Number of customers/ Number of Transactions	Small - 0 / Medium - 0.5 / Large - 1	Data regarding number of transactions for each entity may be obtained from GST databases. Based on this data, suitable thresholds will need to be defined to score an entity as small/medium/large.
Count of attributes of the records processed in last year	N/A	Cannot estimate - 0	
Revenue of firm in the last financial year	Revenue of firm in the last financial year	Small - 0 / Medium - 0.5 / Large - 1	Small <Rs. 75 crore Rs. 75 crore<Medium<Rs 250 Crore Large>Rs.250 crore
Number of entities performing similar function	Number of entities having similar NIC Code	Small - 1 / Medium - 0.5 / Large - 0	Data regarding number of establishments with the same 5 digit NIC code may be obtained from Economic Census. Based on this data, suitable thresholds will need to be defined to score an entity as small/medium/large.

It must be noted that as three of the above variables are assigned a score of 0 for all entities, the maximum score in Year-0 is only 0.6.

Examples of scoring in Year-0

We consider three specific examples in this section to illustrate the use of the indicator-based measurement methodology.

Example 1: Let us consider a small financial institution having about 40 thousand customers, an annual revenue of Rs. 175 crore.

As a financial institution, it is likely to share and access data with other financial institutions like credit bureaus, other banks etc. Hence it is considered to have many inward/outward connections and is given a score of 1 for both those variables. Let us assume it is part of a larger group of companies, and hence is given a score of 1. As it has about 40 thousand customers, a score of 1 is assigned for the total number of data records. Based on criteria laid out above, score of 0.5 is assigned for revenue. Considering that several other similar financial institutions are likely to exist, the model assigns a score of 0 for substitutability.

Based on these scores for individual variables, the overall score for this financial institution is 0.525.

Example 2: Let us consider another example of a large e-Commerce entity with over 2 lakh customers in the past year and Rs. 8,000 crore in revenue.

As an e-Commerce entity, using the list-based approach, it is given a score of 1 for both inward and outward connections. Let us also consider that this entity is part of a larger group which is involved in activities other than e-Commerce and hence is given a score of 1 for the respective variable. It will also be assigned a score of 1 for its number of customers, its revenue and its number of employees. Assuming that a few other players also provide similar e-commerce services, it is assigned a score of 0.5 for substitutability.

Hence, this entity will have a score of 0.575 out of a maximum of 0.6.

Example 3: In a final example, let us consider a small supermarket chain operated by a corporate group. It has reported over 10 lakh transactions in its GST returns, has an annual revenue of Rs. 50 crore and employs 250 people. As a supermarket, it is given a score of 0 for both inward and outward connections. It is assigned a score of 1 based on its large number of transactions. For the variable 'revenue' it scores 0.5. As a supermarket, it is easily substitutable and hence scores 0 for substitutability.

Its total weighted score is thus only 0.325.

It is important to note that these are specific examples and these scores cannot be generalised for the types of firms considered.

Table 3: Examples of Year-0 scoring

Proxy variables for Year 0	**Sub-weight**	**Financial Institution**		**E-commerce**		**Supermarket**	
		Value	**Score**	**Value**	**Score**	**Value**	**Score**
Type of firm (with high in-degrees)	10%	As per list of NIC codes	1	As per list of NIC codes	1	As per list of NIC codes	0
Type of firm (with high out-degrees)	10%	As per list of NIC codes	1	As per list of NIC codes	1	As per list of NIC codes	0
Whether entity is part of larger group structure	10%		1		1		1
Number of customers/ Number of transactions	20%	40,000 customers	1	2,00,000 customers	1	10,00,000 transactions	1
Revenue of firm in the last financial year	5%	Rs. 175 crores	0.5	Rs. 8,000 crores	1	Rs. 50 crores	0.5
Number of entities having similar NIC code	5%	50	0	4	0.5	4	0
Total weighted score			0.525		0.575		0.325

References

- Article 29 Data Protection Working Party. (2017). *Guidelines on Data Protection Impact Assessment and determining whether processing is likely to result in 'a high risk for the purposes of Reg 2016/679'*. European Commission. Brussels: European Commission.
- Ayres, I., & Braithwaite, J. (1992). *Responsive Regulation: Transcending the Deregulation Debate*. Oxford: OUP. Retrieved from http://johnbraithwaite.com/wp-content/uploads/2016/06/Responsive-Regulation-Transce.pdf
- Baldwin, R., & Black, J. (2016). Driving priorities in risk-based regulation: what's the problem? *Journal of Law and Society*, 565-595.
- Basel Committee on Banking Supervision. (2011). *Global Systemically Important Banks: Assessment Methodology and additional loss absorbency requirement*. Bank of International Settlements.
- Basel Committee on Banking Supervision. (2013). *Global systemically important banks: updated assessment methodology and the higher lass absorbency requirement*. Bank of International Settlements.
- Baldwin, R., & Black, J. (2016). *Driving priorities in risk-based regulation: what's the problem?* Journal of Law Society, 565-595.
- Black, J., & Baldwin, R. (2012). When risk-based regulation aims low: Approaches and challenges. *Regulation & Governance*, 2-22.
- Braithwaite, J. (2010). The Essence of Responsive Regulation. *UBC Law Review*, 475-515.
- Carrigan, C., & Poole, L. (2015, June). Structuring Regulators:The Effects of Organizational Design on Regulatory Behavior and Performance. *Penn Program on Regulation*. Philadelphia, Pennsylvania, United States of America. Retrieved from https://www.law.upenn.edu/live/files/4707-carriganpoole-ppr-researchpaper062015pdf
- Committee of Experts on a Data Protection Framework for India. (2017, December 18). White Paper of the Committee of Experts on a Data Protection Framework for India. New Delhi, India: Ministry of Electronics and Information Technology, Government of India. Retrieved July 2018, from http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf
- Competition Commission of India, Government of India. (2018, July 17). *The Competition Act 2002*. Retrieved from Competition Commission of India: https://www.cci.gov.in/sites/default/files/cci_pdf/competitionact2012.pdf
- Directorate of Enforcement, Ministry of Finance. (2018). *About ED*. Retrieved from http://www.enforcementdirectorate.gov.in/about_ed.html?p1=11710211511246704650
- Directorate of Enforcement, Ministry of Finance. (2018, July 17). *Performance of the Enforcement Directorate. Retrieved from Enforcement Directorate*: http://www.enforcementdirectorate.gov.in/functions.html?p1=1186171531818185079
- Dvara Research. (2018). *Draft Data Protection Bill*. Chennai.
- Dvara, Dalberg & CGAP. (2017). *Privacy on the Line*. Mumbai.

- EU General Data Protection Regulation. (2018). Art 35, *General Data Protection Regulation (GDPR)*. Retrieved from intersoft consulting: https://gdpr-info.eu/art-35-gdpr/
- Federal Trade Commission. (2018, March). *Consumer Sentinel Network Data Book 2017*. Retrieved July 2018, from Federal Trade Commission's Website: https://www.ftc.gov/enforcement/consumer-sentinel-network
- Federal Trade Commission. (2018, July 17). *FTC Administrative Staff Manuals*. Retrieved from Federal Trade Commission: https://www.ftc.gov/about-ftc/foia/foia-resources/ftc-administrative-staff-manuals
- Financial Sector Legislative Reforms Commission. (2018, July 17). *Indian Financial Code*. Retrieved from Financial Sector Legislative Reforms Commission: https://dea.gov.in/sites/default/files/fslrc_report_vol2_1.pdf
- Greenleaf, G. (2014). *Asian Data Privacy Laws: Trade and Human Rights Perspective*. London: Oxford University Press.
- Information Commissioner's Office, UK. (2018, July 16). *Data Protection Act 2018*. Retrieved from Information Commissioner's Office: https://ico.org.uk/for-organisations/data-protection-act-2018/
- ITU-infoDev . (2017). Elements for an Effective Regulator. *ITU-infoDev ICT Regulation Toolkit*. Geneva, Switzerland. Retrieved from http://www.ictregulationtoolkit.org/toolkit/6.5#
- Ivec, M., & Braithwaite, V. (2015). *Applications of responsive regulatory theory in Australia and overseas: update*. Canberra: Regulatory Institutions Network.
- Law Commission of India. (2017). *Assessment of Statutory Frameworks of Tribunals in India*. Law Commission of India.
- McGeveran, W. (2016). Friending the Privacy Regulator. *Faculty Articles, University of Minnesota*.
- Meloni, G. (2010). Enabling Regulatory Reform. In OECD, *Making Reform Happen: Lessons from OECD Countries* (pp. 239-267). Brussels: OECD.
- Ministry of Commerce & Industry, Government of India. (2018, July 17). *The Patents (Amendment) Act 2005*. Retrieved from Intellectual Property India: http://www.ipindia.nic.in/index.htm
- Ministry of Statistics and Program Implementation. (2016). *All India Report of 6th Economic Census*. New Delhi.
- Mishkin, B. S. (2018, March). *FTC releases annual report on consumer complaints*. Retrieved July 2018, from Consumer Finance Monitor: https://www.consumerfinancemonitor.com/2018/03/01/ftc-releases-annual-report-on-consumer-complaints/
- Narayanan, A., Toubiana, V., Barocas, S., Nissenbaum, H., & Boneh, D. (2012, February 12). A Critical Look at Decentralized Personal Data Architectures. US. Retrieved from https://arxiv.org/abs/1202.4503

- OECD. (2008). SUMMARY OF DISCUSSIONS ON RISK AND REGULATION AT THE MEETING OF THE GROUP ON REGULATORY POLICY. THE GROUP ON REGULATORY POLICY. OECD.
- OECD. (2013). *Principles for Governance of Regulators*. OECD.
- Office of the Australian Information Commissioner. (2014). *Guide to Undertaking Privacy Impact Assessments*. Sydney: Australian Government. Retrieved from https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments
- Raghavan, M. (2018). Before the Horse Bolts. *Pragati*.
- Reserve Bank of India. (2018, July 17). *Master Circular on Compounding of Contraventions under FEMA 1999*. Retrieved from Reserve Bank of India: https://www.rbi.org.in/Scripts/BS_ViewMasCirculardetails.aspx?id=9873#2
- Restoy, F. (2017, June). *Banking regulation and supervision after the crisis - where are we now, and what lies ahead?* Lisbon. Retrieved from https://www.bis.org/speeches/sp170601.htm
- Rolfe, C. (1997). *Administrative monetary penalties: A tool for ensuring compliance*. Vancouver: West Coast Environmental Law Association.
- Sappington, D. E. (1993, November). Principles of Regulatory Policy Design. Florida, United States: University of Florida. Retrieved from https://pdfs.semanticscholar.org/c32e/7e596b2d6a615fe8e46ce94363b8f3d78c3d.pdf
- Securities and Exchange Board of India. (2018, July 16). Securities and Exchange Board of India (*Informal Guidance Scheme*) 2003. Retrieved from Securities and Exchange Board of India: https://www.sebi.gov.in/informal_guidance.html
- Stephen G Cecchetti. (2011, October 19). *How to cope with the too-big-to-fail problem?* Retrieved from https://www.bis.org/speeches/sp111019.htm
- Task Force on Financial Redress Agency. (2016). *Report of the Task Force on Financial Redress Agency*. New Delhi: Government of India.. Retrieved from https://dea.gov.in/sites/default/files/Report_TaskForce_FRA_26122016.pdf
- Telecom Regulatory Authority of India. (2018, July 17). *Reports on Activities (1 January 2017-31 December 2017)*. Retrieved from Telecom Regulatory Authority of India: https://trai.gov.in/sites/default/files/ActivitiesReportEng07052018.pdf
- UK Information Commissioner's Office. (2017, May). *Management Board terms of reference*. London, UK. Retrieved from https://ico.org.uk/media/about-the-ico/documents/2014132/tor-management-board-201705.pdf
- UK Information Commissioner's Office. (2017). *Protection for Whistleblowers*. Wilmslow : Information Commissioner's Office. Retrieved from https://ico.org.uk/media/report-a-concern/documents/1042550/protection_for_whistle_blowers.pdf
- UK Information Commissioner's Office. (2018). *Working with other bodies*. Retrieved from ICO: https://ico.org.uk/about-the-ico/our-information/working-with-other-bodies/

- United Kingdom Information Commissioner's Office. (2013, August). Data Protection Regulatory Action Policy. *Data Protection Regulatory Action Policy.* London, United Kingdom: United Kingdom Information Commissioner's Office. Retrieved July 13, 2018, from https://ico.org.uk/media/about-the-ico/policies-and-procedures/1853/data-protection-regulatory-action-policy.pdf