Effective Enforcement of a Data Protection Regime

A Model for Risk-Based Supervision Using Responsive Regulatory Tools

Malavika Raghavan, Project Head – Future of Finance Initiative, Dvara Research

DVARA Research

Public Seminar at the National Institute of Public Finance and Policy (NIPFP)
New Delhi, 18 September 2018

Our conversation today

1. Context: Some challenges of data regulation
2. The Working Paper
   - 2.1 Scope and Limitations
   - 2.2 Supervision: Getting to risk-based supervision to act “ex-ante” a breach/compromise of data: A proposal
   - 2.3 Enforcement: A “Responsive Regulation” inspired framework
   - 2.4 Institutional apparatus
3. A brief comparison with the Personal Data Protection Bill 2018
4. Conclusion: Future research and suggestions

DVARA Research

Some challenges of data regulation

1.Context

Some challenges of data regulation

1. Vast regulated space - ubiquitous processing of personal data
2. Contraventions of regime may not manifest or be quantifiable
3. Cross-sectoral effects

DVARA Research

Some challenges of data regulation

- The current approach in India: Ineffective legal protections (IT Act and RSPP Rules) and minimal/no enforcement
- The current approach globally:
  - reliance on penalties and after-the-fact prosecutions
  - self-reported breach notifications
  - complaints/litigations to understand "data harm" (*Chantal Attias, Spokeo line of cases; Cambridge Analytica inquiries etc.)*
- Limited effectiveness in protecting individuals and the system

DVARA Research

Scope and Limitations
Proposals on Supervision and Enforcement
Institutional Apparatus

2.Working Paper

2.1 Scope and limitations

For those of us old enough, we might recall the proclamation of Howard Beale, the veteran news presenter played by Peter Finch in the 1976 classic film *Network*: "Things have got to change. But first, you've gotta get mad! You've got to say, 'I'm as mad as hell, and I'm not going to take this anymore!'" This is where we are with the continuing intrusions upon privacy by governments, intelligence agencies and corporate warlords. It might serve their interests to say that privacy is dead, but it does not serve our interests, the interests of we the people, of a healthy, democratic society. In effect, we have to echo Howard Beale and say that we are as mad as hell and we are not going to take it anymore. Edward Snowden obviously felt this way.

(Wright and De Hert, 2016)

DVARA Research

2.1 Scope

1. Theoretical proposal in response to ineffectiveness of current approaches and the exigencies of our context

2. Reference points (several others as well, cited in Paper)
    - Directorate of Enforcement, Ministry of Finance, Government of India;
    - Report of the Task Force on the Financial Redress Agency (FRA), Ministry of Finance, Government of India.
    - UK Information Commissioner's Office
    - US Federal Trade Commission and US Consumer Financial Protection Bureau

DVARA Research

2.1 Limitations

1. First step rather than definitive model -- early thinking requiring iteration
2. Relational approach, not a ranking
3. Regulatory capacity, resourcing and political will

DVARA Research

2.2 Supervision: A proposal for risk-based supervision “ex-ante” a compromise

Rationale and inspiration

- Risk-based regulation in Privacy: Privacy risk assessment frameworks

Organisation	Dimensions of Risk-based framework		
CNIL, France	Severity*Likelihood		
	Severity: Level of identification of personal data, impact of identification	Likelihood: Vulnerabilities of the supporting asset, capabilities of the risk source	
NIST, USA	Likelihood*Impact		
EU GDPR Article 35*	The Risk that the data action poses to then rights and freedoms of natural persons. For activities categorised as high risk activities there is a Data Protection Impact Assessment.		
*Contained in but not limited to article 35	Article 35 has three prominent dimensions: (i) if the data action deals with automated decision regarding or profiling of natural persons (ii) if it deals with special category data (Article 9) and (iii) systematic monitoring of large public areas.		

2.2 Supervision: A proposal for risk-based supervision “ex-ante” a compromise

Rationale and inspiration

- Risk-based regulation in Finance: The Basel Committee on Banking Supervision’s thinking after the 2008 crisis where firms (i) in maximising their private benefits chose outcomes that were sub-optimal for the system and did not take into account externalities (ii) moral hazard costs of “too big to fail” institutions (FSB, 2010).
- Disorderly failure and significant disruption to the wider financial system & economy.

DVARA Research

2.2 Supervision: A proposal for risk-based supervision “ex-ante” a compromise

BCBS’ Assessment methodology or systemic importance (BCBS, 2011)* (i) indicator based measurement (ii) bucketing (iii) supervisory judgement (iv) periodic review & refinement

Table 1

Indicator-based measurement approach

Category (and weighting)	Individual Indicator	Indicator Weighting
Cross-jurisdictional activity (20%)	Cross-jurisdictional claims	10%
	Cross-jurisdictional liabilities	10%
Size (20%)	Total exposures as defined for use in the Basel III leverage ratio	20%
Interconnectedness (20%)	Intra-financial system assets	6.67%
	Intra-financial system liabilities	6.67%
	Wholesale funding ratio	6.67%
Substitutability (20%)	Assets under custody	6.67%
	Payments cleared and settled through payment systems	6.67%
	Values of underwritten transactions in debt and equity markets	6.67%
Complexity (20%)	OTC derivatives notional value	6.67%
	Level 3 assets	6.67%
	Trading book value and Available for Sale value	6.67%

DVARA Research

(**Revised methodology released in July 2018, under review*)

2.2 Supervision: A proposal for risk-based supervision “ex-ante” a compromise

Our Proposal: Creating an ex-ante “picture” of the market for supervisor using:

1. **Risk based classification** comprising:
    i. a qualitative component accounting for supervisory judgement; and
    ii. quantitative component using multiple indicator-based measurement to arrive at a risk-classification matrix, and
2. **Results of privacy impact assessments** (where available).

DVARA Research

2.2 Supervision: A proposal for risk-based supervision "ex-ante" a compromise

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%

2.3 Enforcement: A "Responsive Regulation" inspired framework

- Responsive Regulation – well developed academic theory (Ayers & Braithwaite, 1992 ; Greenleaf, 2014 (among other works))
- Predicated on:
  - Transparent escalation
  - Accountable exercise of power based on feedback-loops
    - Risk-based supervisory framework assessments
    - Consumer complaints and breach notifications data
    - Media reports
- *"Speak softly and carry a big stick"*

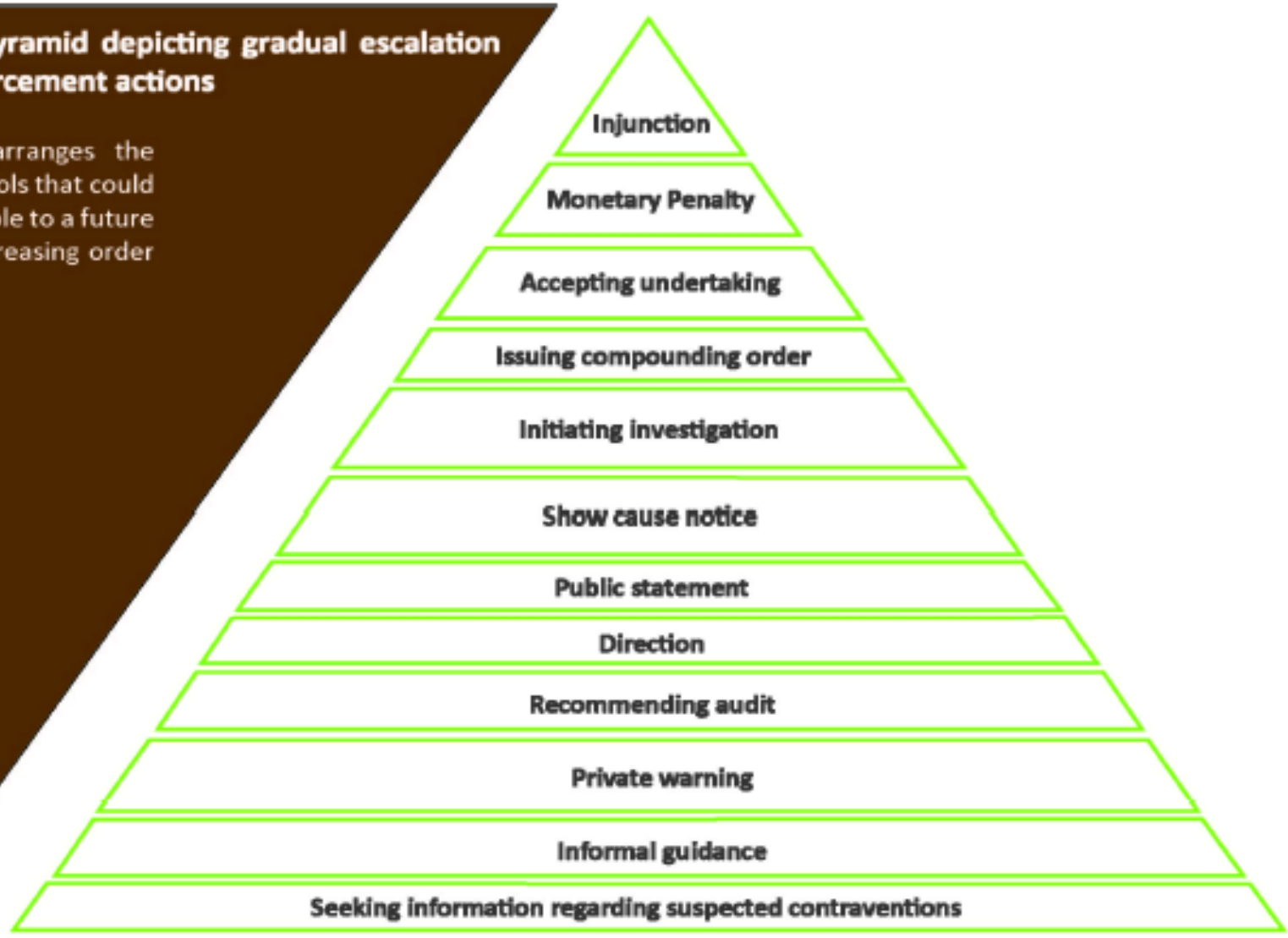
DVARA Research

2.3 Enforcement: A "Responsive Regulation" inspired framework

FIGURE 1: Regulatory pyramid depicting gradual escalation through enforcement actions

Regulatory pyramid depicting gradual escalation through enforcement actions

The pyramid arranges the enforcement tools that could be made available to a future regulator in increasing order of escalation.



2.4 Institutional apparatus

- Chief Data Protection Commissioner accountable to Management Board
- Management Board with independent and full-time members with clear terms of reference
- Transparency through (i) annual report on enforcement actions (ii) monthly reports on complaints data
- Inter-sectoral coordination through MoUs with other regulators/ministries

DVARA Research

2.4 Institutional apparatus

- Internal teams to undertake:
  - Supervision & enforcement,
  - pro-active user protection (through communication and outreach) and complaints management;
  - research and analysis
  - legal expertise;
  - independent quasi-judicial forum at the Authority.
- Regional and zonal presence

DVARA Research

A brief comparison with the Personal Data Protection Bill 2018

3. Comparison

Comparison with Personal Data Protection Bill 2018

1. No mandated regional and zonal presence (s. 49)
2. No consumer complaints database, active complaints management and aligned grievance system
3. No mix of independent and full-time members of Authority (s.50)
4. Accountability measures crucial for truly “responsive” regulation absent
    1. No Management Board structure, crucial for accountability (s. 50)
    2. No publication of annual report on enforcement actions and complaints acted upon and a monthly report on complaints received
5. Significant data fiduciaries (s. 38) does borrow some concepts from working paper when it comes to indicative criteria

DVARA Research

Comparison with Personal Data Protection Bill 2018

6. Enforcement actions and escalation
    - New inclusion: Codes of Practice (s. 61), Criminal Penalties (s. 90-92)
    - No clear feedback loops (from complaints, media reports, supervisory methodology) and clear mechanism to signal escalation
7. Fetters and criteria for discretionary exercise of judgement absent we suggested (Dvara Bill s.23(4)(d)):
    - the nature and seriousness of the contravention of the provisions of the regime;
    - the consequences and impact of contraventions including (i) benefit or unfair advantage gained as a result of the contravention; (ii) loss and harm caused to individuals (iii) repetitive or continuing nature of the contravention; and (iv) other contraventions committed by the entity.

DVARA Research

Future research and suggestions

4. Conclusion

Next Steps

- Fleshing out rationale and motivations in the next draft
- Revisiting weights (and further consideration of factors)
- Further consideration of feedback loops

DVARA Research

Effective Enforcement of a Data Protection Regime

A Model for Risk-Based Supervision Using Responsive Regulatory Tools

Malavika Raghavan, Project Head – Future of Finance Initiative, Dvara Research

DVARA Research

Public Seminar at the National Institute of Public Finance and Policy (NIPFP)
New Delhi, 18 September 2018

References

- 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.
- Financial Stability Board. (2010). *Reducing the moral hazard posed by systemically important financial institutions.*
- Wright, D and De Hert, P (2016) Introduction to Enforcing Privacy in *Enforcing Privacy: Regulatory, Legal and Technological Approaches (Law, Governance and Technology Book Series, Volume 25),* Basel: Springer, Cham.

DVARA Research