The Dialogue™
INFORM ENGAGE IDEATE

INVEST INDIA
NATIONAL INVESTMENT PROMOTION
& FACILITATION AGENCY

RESEARCH PAPER

PRIVACY TECHNOLOGIES IN INDIA

STRATEGIES TO ENHANCE THE ECOSYSTEM

RESEARCH PAPER

PRIVACY TECHNOLOGIES IN INDIA
STRATEGIES TO ENHANCE THE ECOSYSTEM

Authors

The Dialogue™ - Kamesh Shekar, Kazim Rizvi, Sreyan Chatterjee, Eshani Vaidya, Saksham Malik, Karthik Venkatesh

Invest India - Simran Khurana, Soumil Gupta

Copyeditor Akriti Jayant
Designer Shivam Kulshrestha

The Dialogue™ is a public policy think tank with a vision to drive a progressive narrative in India's policy discourse. Founded in 2017, we believe in facilitating well-researched policy debates at various levels to help develop a more informed citizenry, on areas around technology and development issues. The Dialogue™ has been ranked as the world's Top 10 think tanks to watch out for, by the Think Tank and Civil Societies Programme (TTCSP), University of Pennsylvania in their 2020 and 2021 rankings.

Invest India is the National Investment Promotion and Facilitation Agency of India, set up as a non-profit venture under the aegis of Department of Industrial Policy & Promotion, Ministry of Commerce and Industry, Government of India. It facilitates and empowers all investors under the 'Make in India' initiative to establish, operate and expand their businesses in India.

For more information
https://thedialogue.com | https://investindia.gov.in

Suggested Citation
Shekar, K., Rizvi, K., Chatterjee, S., Vaidya, E., Malik, S., Venkatesh, K., Khurana, S., & Gupta, S. (2023, July). Privacy Technologies in India: Strategies to Enhance the Ecosystem. The Dialogue™ & Invest India.

Catalogue No.
TD/PDG/RP/0723/02

Publication Date
July 20, 2023

Disclaimer
The facts and information in this report may be reproduced only after giving due attribution to the authors, The Dialogue™, and Invest India.

ACKNOWLEDGEMENT

We would like to extend our sincere gratitude to Ms Nivruti Rai, CEO & MD, Invest India; Mr Gaurav Sishodia, Cluster Lead & VP (ESDM-TMT, Invest India; Mr Anuj Kapur, Senior Director & Head of India Region, Invest India; Mr Uday Wadhwa, Investment Specialist, Invest India for extending their support to the paper. We also extend our gratitude to Mr Anshu Sharma, Co-founder & CEO, Skyflow, Subhashish Bhadra, Head of Corporate Development, Klub, and Anand Venkatanaryanan, DeepStrat, for their invaluable input to the paper.

We also extend our gratitude to Akriti Jayant for providing copyediting support and Shivam Kulshrestha for his design support to this report.

TABLE OF CONTENTS

Foreword - Ms. Rama Vedashree **1**

Executive Summary **2**

1. Introduction **10**

2. Status Quo of Privacy Technology **11**

3. Privacy Technology – A Landscape **12**

3.1. Mapping the growth of PETs across the data lifecycle **14**

3.1.1. Data collection **15**

3.1.2. Data retention **17**

3.1.3. Data structuring **18**

3.1.4. Data transfers **18**

3.1.5. Data processing **19**

3.1.6. Data expunction **21**

3.2. Evolution of Privacy Preserving Technology **22**

4. Structural Challenges for Privacy Technology **23**

4.1. The Trend of Legal Endogeneity **23**

4.2. Limits of Technological Outsourcing **24**

4.2.1. Power Asymmetries **26**

4.2.2. Narrowing Privacy Law **26**

4.2.3. Erosion of Expertise **26**

4.2.4. Lack of Accountability **26**

5. Operational Challenges for Privacy Technology **27**

5.1. Demand-side challenges **27**

5.1.1. Lack of a privacy-centric culture **27**

5.1.2. Limited focus on creating value out of data **29**

5.1.3. Low demand from users **30**

5.1.4. Limited awareness of business incentives **30**

5.1.5. Budgetary restrictions **31**

5.1.6. Gap in knowledge and internal processes **32**

5.2. Supply-side challenges **32**

5.2.1. Lack of consensus on theoretical frameworks **33**

5.2.2. Shifts in regulatory landscape **34**

5.2.3. Challenges pertaining to the growth of Artificial Intelligence **34**

6. The Way Forward and Recommendations **36**
6.1. Government **36**
6.1.1. Regulatory enablers **36**
6.1.2. Incentives **37**
6.1.3. Fiscal support **37**
6.1.4. Competence building **39**
6.2. Private Enterprises **40**
6.2.1. A shift in cultural factors **40**
6.2.2. Internal processes **42**
6.2.3. Budgetary restrictions **42**
6.3. Investors **43**
6.3.1. Privacy protection as a value addition **43**
6.3.2. Growth of context-appropriate privacy-tech start-ups **44**
6.4. Civil Society **45**
7. A framework to understand privacy-technology readiness of firms **45**
7.1. The Data Balance Sheet **46**
7.2. Technical Strategy **50**
7.2.1. Data Enumeration **50**
7.2.2. Data Flow Mapping **51**
7.2.3. Data Categorisation **52**
7.2.4. Data Access Control **53**
7.2.5 Data Convergence **55**
Conclusion **56**

List of Figures:

Figure 1: Way Forward
Figure 2: Way Forward - Government
Figure 3: Way Forward - Private Enterprises
Figure 4: Way Forward - Investors
Figure 5: Way Forward - Civil Society
Figure 6: Mapping PETs

List of Figures:

Box 1: Privacy-enhancing Technology: Account Aggregator System
Box 2: Time V alue of Data
Box 3: Dashboard View
Box 4: Lossy Compression

List of Tables:

Table 1: PETs - Data Collection
Table 2: PETs - Data Retention
Table 3: PETs - Data Structuring
Table 4: PETs - Data Transfers
Table 5: PETs - Data Processing
Table 6: PETs - Data Expunction
Table 7: Indicative List of Data Categorisation Table 8: Indicative
Mapping of Access Control

ABBREVIATIONS

Abbreviation	Definition
AA	Account Aggregator(s)
AI	Artificial Intelligence
BIS	Bureau of Indian Standards
DEPA	Data Empowerment and Protection Architecture
DPDPB 2022	Digital Personal Data Protection Bill 2022
DSD	Dispute Systems Design
E2EE	End to End Encryption
EU	European Union
GDPR	General Data Protection Regulation
HIPAA	The Health Insurance Portability and Accountability Act of 1996 (United States)
ID	Identification Document
IIT	Indian Institute of Technology
IoT	Internet of Things
IT	Information Technology
IT/ITeS	Information Technology/Information Technology enabled Services
ML	Machine Learning
MSME	Micro, Small and Medium Enterprises
SME	Small and Medium Enterprises
NASSCOM	The National Association of Software and Service Companies
NBFC	Non-Banking Financial Company
PET	Privacy Enhancing Technology
PII	Personally Identifiable Information
PPT	Privacy Preserving Technology

Privacy Tech	Privacy Technology
RBI	Reserve Bank of India
SDK	Software Development Kit
SIEM	Security Information and Event Management
SMEs	Small and Medium Enterprises
TRL	Technology Readiness Level

FOREWORD
MS. RAMA VEDASHREE

India @75 has been scripting a new phase of accelerated digitalization, and our pioneering efforts at digital innovation and technology-enabled inclusion and socio-economic growth are garnering global attention. The technology industry, which has been driving digital transformation for enterprises worldwide, is now a $245 Billion Industry and consistently clocking double-digit growth. Public Service delivery both at the states and Centre, is architected for scalable technology platforms serving citizens over multiple channels. Digital is embedded in Society, both urban and rural, and consumers prefer digital in financial services, shopping online, entertainment, education and skills development, and healthcare. This all-pervasive shift to digital has led to expanding online digital footprints of all segments of our society. Data-driven innovation is central to every business's growth; emerging technologies and AI are key to offering personalised services to consumers.

As we move forward, I believe to realise the maximum potential of digital and data-led innovation, it is essential for businesses to consider trust on an even keel with other business considerations. To build consumer trust, businesses must move from a compliance focus to privacy, being considered a value proposition and competitive advantage. As businesses craft their enterprise data strategies centred around consumer trust, technology solutions for implementing privacy have gained momentum. The Global Privacy Technology vendor landscape now spans 350 plus companies, and India has also seen the nascent privacy-tech ecosystem grow in the last three years. 'Think Privacy Think Technology' is an initiative that was taken up by the Data Security Council of India to grow the privacy startup ecosystem.

The government of India is in the process of enacting legislation for securing digital spaces like the upcoming data protection bill. However, enforcing and implementing a comprehensive data protection and privacy regime with the continually changing technology landscape and billion-plus consumers/citizens across sectors is daunting for both regulators and industry. Therefore, I believe Privacy Enabling Technologies can help both government and businesses in their privacy journey and make their digital services and products privacy aware by design.

As privacy technologies are at their nascent stage in India, I want to compliment The Dialogue and Invest India for this timely paper on "Privacy Technologies in India: Strategies to Enhance the Ecosystem", which discusses the privacy technology landscape of India, its operational challenges, and the way forward. The paper ties the demand-side, supply-side and technological facets together and provides a holistic perspective on the role of various stakeholders in enhancing the market for privacy technologies in India.

I believe the way forward strategies mapped in this paper to some of the critical actors, such as government, investors, private enterprises, and civil society, is a step in the right direction and could aid the evolution of the privacy technologies ecosystem in India. As India has made rapid strides in her digital transformation journey, it's time we give attention to the innovation and growth of privacy technologies and their adoption by both government and business. I do hope this paper helps evangelise with all stakeholders, the importance of privacy-tech in rolling out robust privacy programs.

EXECUTIVE SUMMARY

The protection of the individual's right to privacy has occupied center stage in recent years, while the focus, earlier, was on cybersecurity. A specific approach towards protecting networks, overall servers and systems, cybersecurity stands distinct from privacy technology ('privacy-tech'), focusing on the individuals' right to privacy. The first stage of the evolution of privacy-tech was marked by the need to comply with data protection legislation being enacted across the globe. A notable development was the competitive advantage data fiduciaries could secure by adopting privacy-tech. This inspired a shift from privacy- tech fulfilling mere compliance roles to a more privacy-first culture prioritizing individual privacy and security.

EVOLUTION OF PRIVACY TECHNOLOGY

The earliest developments in privacy- tech were the privacy-by-design principles introduced in the 1990s. Subsequently, privacy-enhancing technologies evolved due to the enactment of global data protection regulations, such as the omnibus data protection regime like the General Data Protection Regulation (GDPR in the European Union. These regulations focus primarily on fiduciaries complying with the relevant provisions rather than building a holistic privacy- tech culture. However, with increasing consumer-led demand, services have expanded into building technology solutions that expand on pre-existing privacy- tech solutions, thereby increasing the degree of security offered; (dubbed by some as Privacy Enhancing Technologies and adopting services that guarantee user privacy in a multi-layer format (often dubbed Privacy-Preserving Technologies.

Therefore, in theory, while multiple PETs might be deployed to secure individual data, a single PPT is meant to serve the same purpose. The technology-readiness level, i.e. the degree of maturity of these technologies, is relatively low, particularly in the Global South. This makes seamless adoption a challenge. For instance, one of the most common debates in the South is the need for encryption. Encryption technologies provide a necessary but limited first step towards creating an ecosystem that protects an individual's privacy across the data lifecycle. Privacy- tech vendors aim to provide solutions that protect one's privacy while maximising the value of data throughout the business.

CHALLENGES IN THE GLOBAL SOUTH

Privacy- tech in the Global South is notably distinct from the markets in developed countries. In India specifically, for instance, the industry is relatively new and often absent from several businesses' work cultures. An understanding of privacy, experts argue, requires one to consider the management of users' expectations, their desire for obscurity and the need for trust. **Our report highlights the structural challenges into two broad buckets—the trend of legal endogeneity and the limits of technological outsourcing.** With privacy regulations being developed in several jurisdictions, its regulatory landscape has become increasingly more complex. As a result of this, the businesses face most challenge in interpreting the privacy law. It is important that in interpreting the law, the technology solution does not occupy centre stage. The danger of such a focus is that the impact of data protection regulations will be diluted during implementation. Ensuring that privacy outcomes for individuals are centred requires collaboration between the in-house privacy teams of companies with those providing privacy technology. As discussed in the report, the lack of a privacy-first culture poses a significant hurdle towards reaching that goal.

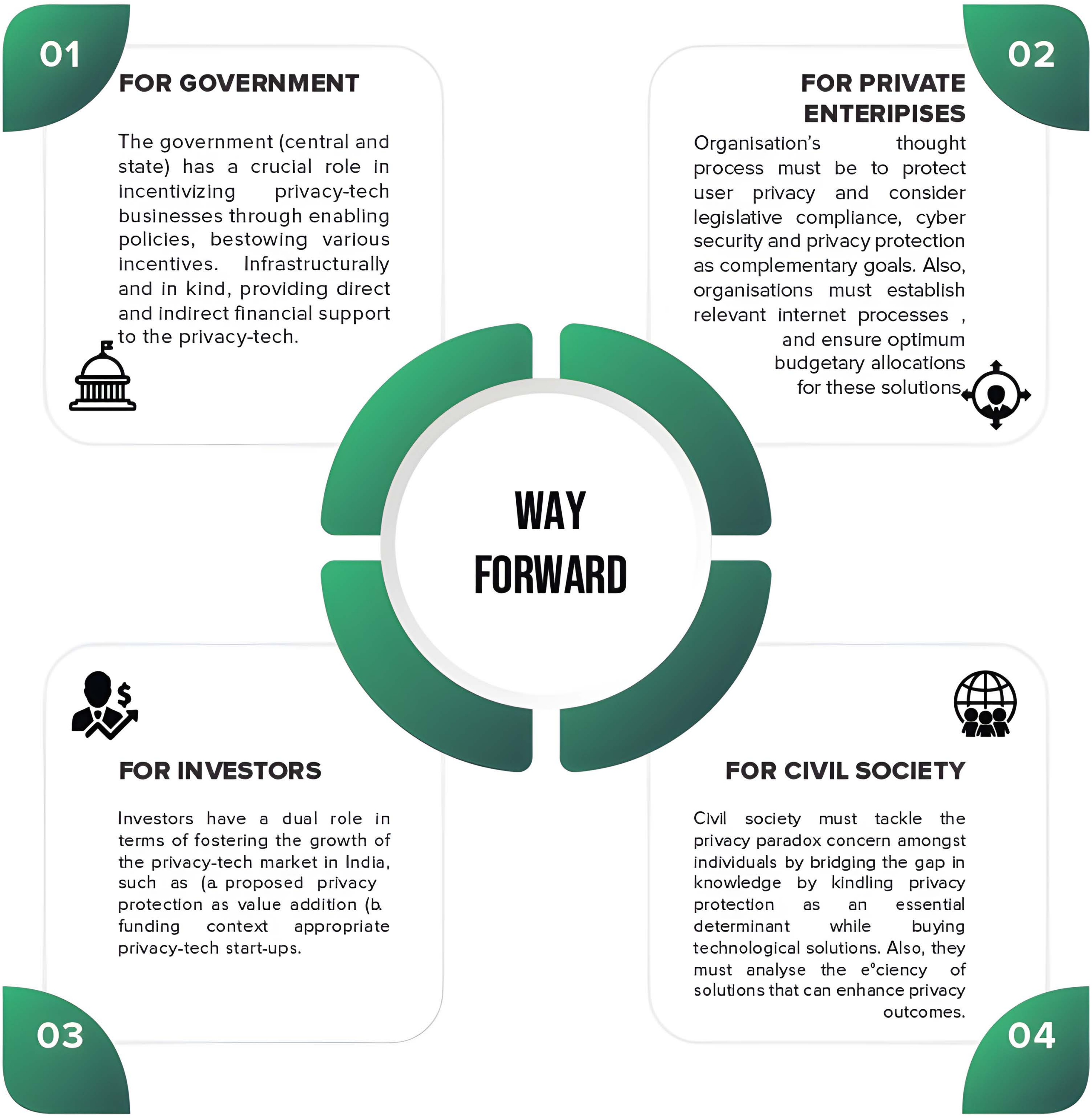
OPERATIONAL CHALLENGES

Bottlenecks identified on the demand side include low user demand, limited awareness of business incentives, budgetary restrictions, and a knowledge gap within internal processes. The supply-side challenges include a lack of consensus on theoretical frameworks and frequent shifts in the regulatory landscape. The result is that most companies adopting privacy technology in India are limited to cybersecurity solutions. Those operating in the Global North often have to comply with the GDPR, which, in turn, accelerates the adoption of privacy technologies. In order to understand India's transition towards chartering a privacy-safe environment, it is important to discuss the role of the legislature, executive, and judiciary in building a free and fair digital economy that respects informational privacy.

Our study tries to understand the reasons behind the slow uptake of privacy technologies in India to provide action points for each major stakeholder. The level of trust that needs to be established will vary based on the nature of the data being shared, for instance, health data must be accorded a higher degree of protection. Our objective has been to study the expectations of each stakeholder within the privacy-tech ecosystem. This has been done with a particular focus on the industry and its challenges in establishing a privacy-first culture.

WAY FORWARD

Figure 1: Way Forward



01

FOR GOVERNMENT

The government (central and state) has a crucial role in incentivizing privacy-tech businesses through enabling policies, bestowing various incentives. Infrastructurally and in kind, providing direct and indirect financial support to the privacy-tech.

02

FOR PRIVATE ENTERIPISES

Organisation's thought process must be to protect user privacy and consider legislative compliance, cyber security and privacy protection as complementary goals. Also, organisations must establish relevant internet processes , and ensure optimum budgetary allocations for these solutions.

WAY FORWARD

03

FOR INVESTORS

Investors have a dual role in terms of fostering the growth of the privacy-tech market in India, such as (a proposed privacy protection as value addition (b. funding context appropriate privacy-tech start-ups.

04

FOR CIVIL SOCIETY

Civil society must tackle the privacy paradox concern amongst individuals by bridging the gap in knowledge by kindling privacy protection as an essential determinant while buying technological solutions. Also, they must analyse the efficiency of solutions that can enhance privacy outcomes.

1. Way Forward: Government

Our findings overwhelmingly point to the need for regulatory support. The legislation will not only be a critical stepping stone towards creating standardized processes, including a taxonomy, but the need to comply will also have a positive effect on the privacy technology industry. For instance, data classification or labelling does not have any accepted industry standards that are relied upon in India. Governments can also aid privacy-tech businesses by developing clear definitions for key terminologies, like privacy-preserving technologies, and privacy enhancing technologies, in addition to defining the regulatory thresholds for compliance.

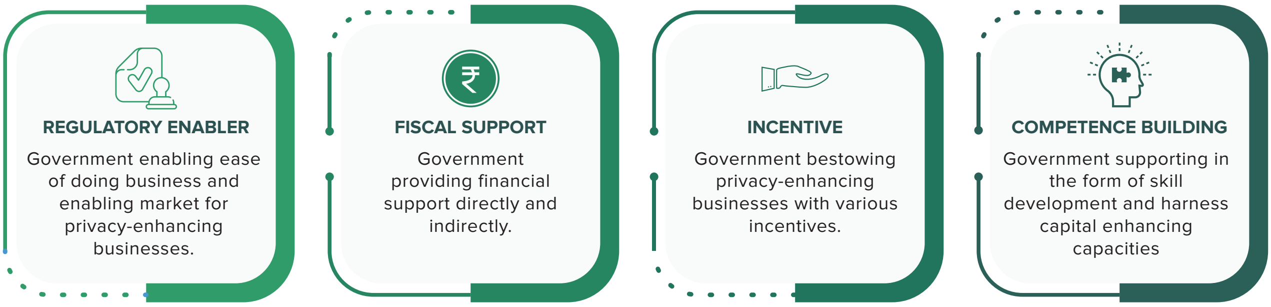
Regulatory enablers will also enable ease of doing privacy-tech business through the provisions enhancing regulatory requirements, compliance, and due diligence. With adequate support given to those within the privacy technology industry, the positive knock-on effect will be felt across other critical industries, such as digital healthcare and fintech. Efforts in this regard could include regulatory sandboxes and provide adequate intellectual property rights mechanisms. For instance, privacy could be incorporated as an element in pre-investment due diligence. The central and state governments already use the sandbox mechanism, in addition to regulatory bodies like the Reserve Bank of India.

Enabling recognition by the Department for Promotion of Industry and Internal Trade will also allow start-ups to get various benefits. State-backed incentives can include those granted infrastructurally or as indirect monetary benefits to enable innovation. Going beyond the basic provisions of fiscal support, the government can grant access to existing infrastructure, such as start-up parks, IT parks, innovation hubs, etc., set up by various state governments. Providing monitoring support and knowledge-sharing mechanisms through a holistic mentoring facility, for instance, would allow for a better understanding of the technologies themselves. For instance, a separate nodal agency for privacy-tech backed by the Start-up India initiative could act as a single window for clearance for exemptions, incentives, and grievance redressal.

Summary of Recommendations:

A legislation can enhance the privacy-tech ecosystem by providing/provisioning the following:

- A standardized taxonomy;
- Sandbox mechanisms can be incorporated across industries;
- Recognition by DPIIT could allow for the institutionalization of fiscal benefits, in addition to increased investment in physical infrastructure; and
- An independent nodal agency could improve grievance redressal systems and promote awareness, thus establishing a privacy-first culture.



REGULATORY ENABLER

Government enabling ease of doing business and enabling market for privacy-enhancing businesses.

FISCAL SUPPORT

Government providing financial support directly and indirectly.

INCENTIVE

Government bestowing privacy-enhancing businesses with various incentives.

COMPETENCE BUILDING

Government supporting in the form of skill development and harness capital enhancing capacities

Figure 2: Way Forward - Government

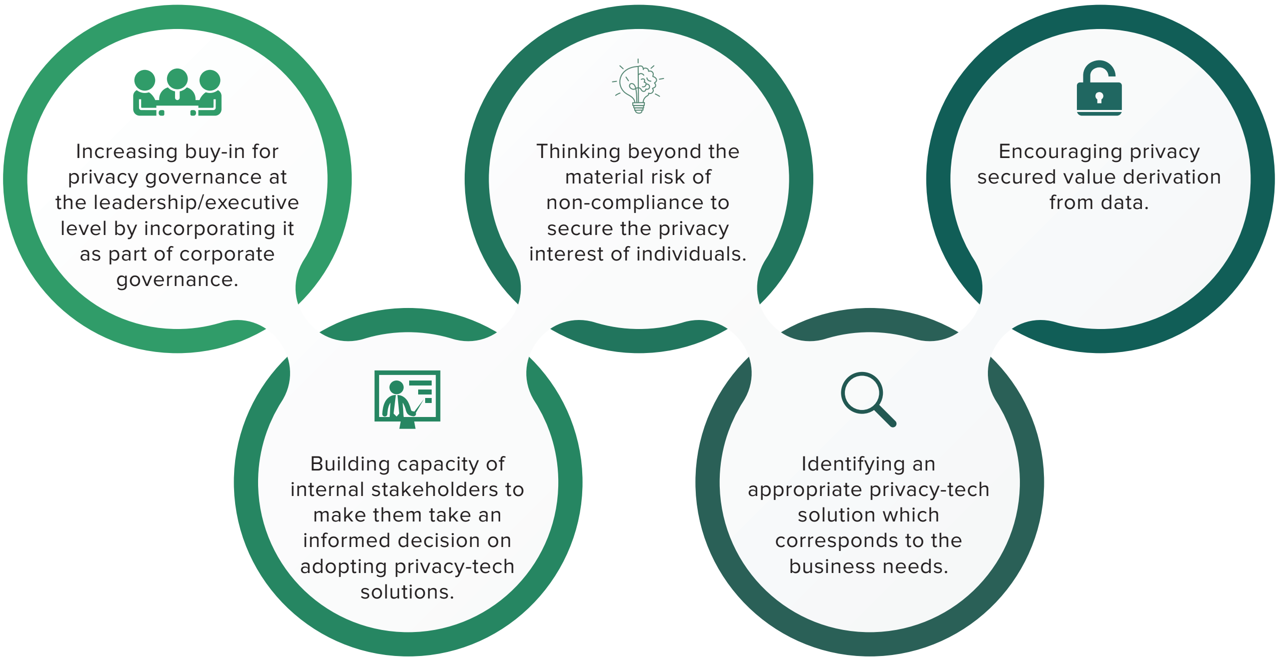
2. Way Forward: Private Enterprises

Privacy organizations play a critical role in building and supporting a privacy-first culture that prioritizes user privacy protection. Private enterprises must invest more resources in creating a privacy-centric culture, which includes considering legislative compliance, cyber security, and privacy protection as complementary goals. For instance, data security and privacy can be a part of corporate governance strategies, and sub-committees can be created to conduct regular assessments and assign a privacy budget. To make informed decisions about adopting the right privacy technology, companies must build internal capacities first. Training cannot be reduced to a mere box-ticking exercise but should help employees realize the practical value of privacy-tech solutions. Increasing the awareness of privacy-tech solutions or introducing a team focused on protecting user privacy will ensure that there is a comprehensive view of the company requirements, and that the technology can be meaningfully utilised. Technology that can affordably protect user privacy must be given an increased focus on privacy budgets.

Summary of Recommendations:

Building internal capacities must be prioritised. This includes the following action points:

- Establish training programmes that allow for a practical understanding of the importance of privacy-tech and the manner in which it functions;
- The need for privacy-tech must also be reflected in financial decision-making for which sub-committees can be formed.
- Legislative compliance must not be the only goal, and the fiscal benefits (such as attracting more FDI must be given their due.



Increasing buy-in for privacy governance at the leadership/executive level by incorporating it as part of corporate governance.

Thinking beyond the material risk of non-compliance to secure the privacy interest of individuals.

Encouraging privacy secured value derivation from data.

Building capacity of internal stakeholders to make them take an informed decision on adopting privacy-tech solutions.

Identifying an appropriate privacy-tech solution which corresponds to the business needs.

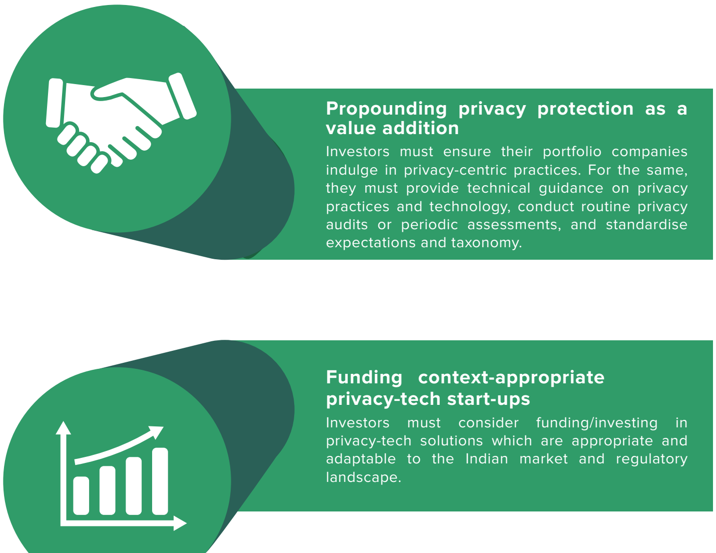
Figure 3: Way Forward - Private Enterprises

3. Way Forward: Investors

Privacy-tech solutions also assign investors an important role where they can choose companies that value privacy, and they can facilitate the development of privacy -tech by investing in solutions that are fit for the Indian market. This would include viewing privacy protection as a value addition rather than a basic hygiene criterion focussed on regulatory compliance. A more strategic approach must be adopted to provide technical guidance on privacy practices and technology, routine privacy audits or periodic assessments. Investors can also facilitate the development of a standardised taxonomy and metrics for decision-making at the board level that can include privacy as a vital cog of the business model itself. This will ensure that potential portfolio companies can derive optimum value out of data in a sustainable and privacy-centric manner.

Summary of Recommendations:

- Investors must value TRL, data protection practices (beyond individual privacy) and the inclusion of privacy technology in key budgetary decisions above simple checkbox exercises for regulatory compliance.
- Invest in companies focussing on building a privacy-first culture—this can be done by a dynamic evaluation process that studies TRL.
- Regulatory compliance, while important, cannot be granted singular focus by investors.



Propounding privacy protection as a value addition

Investors must ensure their portfolio companies indulge in privacy-centric practices. For the same, they must provide technical guidance on privacy practices and technology, conduct routine privacy audits or periodic assessments, and standardise expectations and taxonomy.

Funding context-appropriate privacy-tech start-ups

Investors must consider funding/investing in privacy-tech solutions which are appropriate and adaptable to the Indian market and regulatory landscape.

Figure 4: Way Forward - Investor

4. Way Forward: Civil Society

Lastly, civil society has a dual objective–encouraging the shift towards making privacy protection an important determinant while purchasing technology; and working towards the resolution of the privacy paradox. This can be done by producing literature and tools aimed at explaining concepts pertaining to privacy. For instance, developing impact assessment reports or tools to evaluate the technological readiness level of various privacy technologies in the country will help create a more informed consumer base. There is a need to analyse the efficiency of existing solutions to identify points of vulnerability and new improvement areas.

Summary of Recommendations:

Civil society plays a crucial role in identifying the bottlenecks in the industry and the need for increased consumer privacy. The following action points are therefore critical to adopt:

- Work must be targeted towards awareness of the need for data protection beyond individual privacy. This must be done within the industry and at the consumer levels.
- Conversations with the Government (closed door and otherwise) can ensure that stakeholder expectations are addressed in legislation.
- Civil society plays a crucial role in identifying incentives for investors and conveying the same to policymakers.
- Can participate in developing a robust audit mechanism, including inputs on Impact Assessment Reports.
- Development of a TRL report will not only provide investors with a valuable assessment toolkit, but will also allow consumers to make informed decisions.

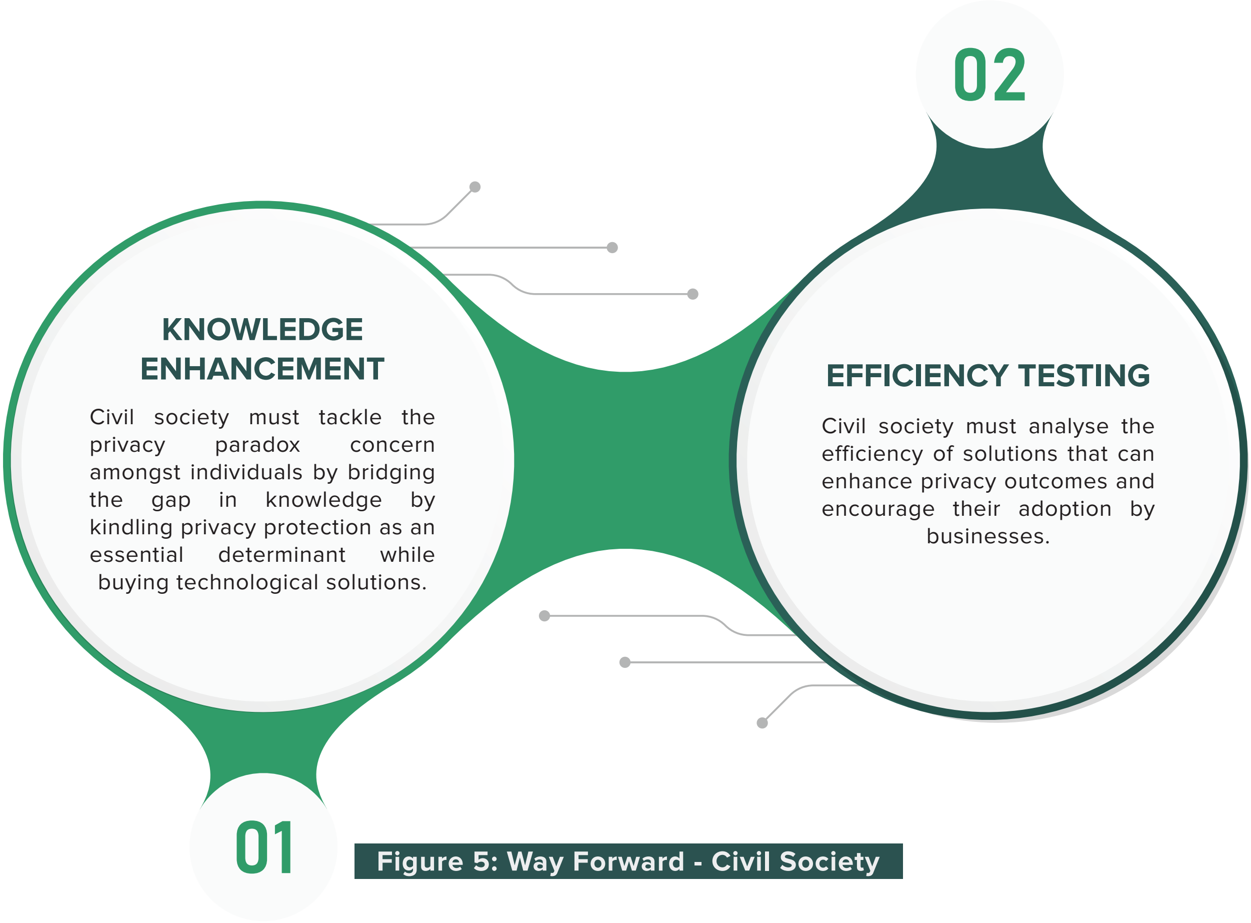

02
KNOWLEDGE ENHANCEMENT
Civil society must tackle the privacy paradox concern amongst individuals by bridging the gap in knowledge by kindling privacy protection as an essential determinant while buying technological solutions.
EFFICIENCY TESTING
Civil society must analyse the efficiency of solutions that can enhance privacy outcomes and encourage their adoption by businesses.
01

Figure 5: Way Forward - Civil Society

CONCLUSION

India has made a remarkable journey towards creating a comprehensive data protection regulation for the country to secure the right to privacy of individuals. Towards this, the report is a timely effort to lay out the national strategy for enhancing privacy-tech in India, which could complement the efforts taken by the government towards establishing a privacy-first culture in India. The report takes one step further from considering privacy technology as a compliance instrument and suggests means through which the technology could establish a culture where privacy is considered a value proposition through concerted efforts by various stakeholders in India. The holistic approach adopted by the report tries to take a bottom-up approach where we emphasise the efforts needed from every stakeholder from the grassroots, i.e., individuals to businesses and government. Our strategies try to create awareness among individuals and incentive structure to follow by the investors, which would propel businesses to adopt privacy-tech, boosting the market for the same.

1 INTRODUCTION

Internet penetration in India is witnessing a surge, with the COVID-19 pandemic-induced lockdowns accelerating the trend of consumers adopting services in the digital ecosystem. The internet penetration rate in India stood at 48.7% at the start of 2023[1], and information technology spending is expected to have increased by 2.6% in 2023 compared to 2022[2]. This rise in the utilisation of digital services also led to increased risks of exclusion in addition to the increase in potential privacy harms. This has led to a shift in the privacy culture, creating a more individual focus, i.e., protecting personal data. The General Data Protection Regulation defines personal data as 'any information relating to an identified or identifiable natural person ('data subject'; an identifiable natural person can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.'

Risk-based assessments may also create a category of 'sensitive personal data' requiring additional protection. For instance, the personal data of minors that may be collected through online education services or health data is often classified as such.

The growing importance of one's right to privacy was marked by the Puttaswamy Judgement in 2017[3]. The Hon'ble Supreme Court declared the right to privacy as a fundamental right under Article 21 of the Indian Constitution. The recent draft of the Digital Personal Data Protection Bill, 2022 (DPDPB, 2022 also seeks to 'recognise the right of individuals to protect their personal data'. The intensification of data practices has also pushed India's digitisation ambitions to the front seat, with NASSCOM (an IT/ITeS industry body estimating that data and Artificial Intelligence (AI will generate over $500 billion in value by 2025[4]. While data is one of the primary drivers of India's trillion-dollar digital economy vision[5], the call for securing informational privacy has become louder not just on the demand side, but also on the supply side. The introduction of the Digital Personal Data Protection Bill, 2022 is a step towards formalising the principles introduced and creating a compliance-driven market.

With the introduction of the GDPR, the first phase of privacy-preserving technologies was aimed at fulfilling business entities' immediate compliance needs[6]. Subsequently, there has been a narrative shift towards a 'privacy-first' culture on a global scale. Reflecting this shift, in the past few years, businesses have been taking the initiative and deploying novel privacy technologies (privacy-tech) that go a step further than legal compliance. Privacy technologies, therefore, aim to design novel systems where privacy is improved at the get-go while also improving privacy in existing systems[7].

[1] Kemp, S. (2023, February 13). Digital 2023: India — DataReportal – Global Digital Insights. DataReportal. Retrieved July 1, 2023, from https://datareportal.com/reports/digital-2023-india Gartner Forecasts India IT Spending to Grow 2.6% in 2023. (2022, November 14).

[2] Gartner. Retrieved July 1, 2023, from https://www.gartner.com/en/newsroom/press-releases/2022-11-14-india-it-spending-forecast-2023

[3] Justice K. S. Puttaswamy (Retd.) and Anr. vs Union Of India And Ors. AIR 2017 SC 4161

[4] Unlocking Value from Data and AI – The India Opportunity. (2020). Retrieved from NASSCOM: https://community.nasscom.in/system/files/report/28219-final-nasscom-report-onscreen-2.pdf

As privacy technologies are nascent in India, in this paper we discuss their growth, journey, and challenges the industry faces. In Chapter 2, we analyse the status quo of privacy technology in India by discussing the trends in privacy technology, including the focus on data management and process orchestration, before briefly discussing factors that impact the industry's growth. Chapter 3 thoroughly explores the privacy technology landscape, including the journey of Privacy Enhancing Technologies (PETs to Privacy Preserving Technologies. This chapter provides a comprehensive map of various PETs present at various stages of the data lifecycle, from data collection to data expunction. It also traces the evolution of PPTs, their scope as well as their importance for privacy compliance. Chapter 4 discusses the structural and operational challenges of privacy technology in addition to various demand and supply challenges impacting the uptake and growth of privacy technology in India.

In order to recommend grounded solutions, we studied the expectations of various stakeholders within the industry. Chapter 4 & 5 of the paper, therefore, proposes various recommendations for the government, private enterprises, investors, and civil society to ensure the growth of privacy-tech solutions and consequent protection of users' privacy interests. Lastly, Chapter 6 the paper proposes a framework to understand the technology readiness level (TRL of firms. The framework provides a zero-to-one flow required to successfully manage a typical data-intensive company in an environment where data protection is a legal obligation and a user expectation.

2 STATUS QUO OF PRIVACY TECHNOLOGY

The market for privacy technology has been largely focused on developing cybersecurity solutions. The rise in data breaches led data protection and security practices to become a part of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011. Currently, the technologies focus on three key areas: personal data management and governance solutions, risk management and compliance, and process orchestration[8]. Personal data management solutions allow companies to store, retain and use their data effectively and securely. Automated data discovery tools, for example, would be a personal data management solution. Process orchestration solutions allow automation and standardisation of processes to improve efficiency. For example, automatic responses to users requesting access to their personal data. Technology can also ease cross-border compliance processes with business entities often operating in multiple jurisdictions.

[5] India’s Trillion Dollar Digital Opportunity. (2019). Retrieved from MEITY: https://www.meity.gov.in/writereaddata/files/india_trillion-dollar_digital_opportunity.pdf

[6] Timan, T. & Z. Á. Mann, Data Protection in the era of artificial intelligence. Trends, existing solutions and recommendations for privacy-preserving technologies, Big Data Value Association, Retrieved on January 16, 2022 from https://www.bdva.eu/sites/default/files/Data%20protection%20in%20the%20era%20of%20big%20data%20for%20artificial%20intelligence_BDVA_FINAL.pdf

[7] Timan, T. & Z. Á. Mann, Data Protection in the era of artificial intelligence. Trends, existing solutions and recommendations for privacy-preserving technologies, Big Data Value Association, Retrieved on January 16, 2022 from https://www.bdva.eu/sites/default/files/Data%20protection%20in%20the%20era%20of%20big%20data%20for%20artificial%20intelligence_BDVA_FINAL.pdf

[8] Privacy Technology: What’s Next?, KPMG International Retrieved on January 8, 2022 from https://assets.kpmg/content/dam/kpmg/xx/pdf/2021/05/privacy-technology-whats-next.pdf

While the status quo shows privacy technology tilted towards the supply-side management of processes, operations, and compliance, studies have shown that in addition to this, companies must develop privacy-centric designs to appeal to consumers. Now more than ever, consumers are inclined to choose products with a better privacy rating[9]. With the latest DPDPB, 2022, it is likely that the obligations of data fiduciaries will be expanded. Therefore, with the importance of a ‘privacy-first’ strategy increasing, companies must find a way to operationalise the necessary technology effectively and consistently for data security and privacy.

However, the privacy culture in India is relatively new and is growing. While there is a steady movement toward privacy-first culture, however, there is still a long way to go in terms of imbibing the same at the organisational level where businesses do have a growing emphasis on the same. Therefore, in the short run, businesses focus on building a data extraction culture with less focus on achieving a positive sum game in the long run where privacy and consumer protection are considered as a value proposition, through innovating on privacy safeguards.[10]

Even though risk management solutions seek higher uptake rates from businesses, operationalising these solutions has proven to be an uphill task. Data classification and labelling do not have any accepted industry practices or standards. Classification is extremely important because the treatment of different kinds of data will vary based on this risk-based assessment. However, the absence of trained personnel and the enabling infrastructure slows the process down significantly. Small and Medium Enterprises (SMEs), in particular, do not have the resources to employ people dedicated to managing privacy technology within the company. On the other end of the spectrum, businesses with requisite resources face longer sales cycles because several new technologies employ new personnel, such as employees exclusively allocating budget for buyers.

Moreover, privacy technology solutions can also rarely operate in silos. Encryption technology, for example, is a vital product for cybersecurity but is insufficient. To protect data throughout its lifecycle and for regulatory compliance, a company will have to deploy various technologies that can work in sync with each other. These technical solutions, therefore, attempt to preserve privacy throughout the lifecycle of data, at the source, during the processing of data or at the outcome of data analysis or all three.

3 PRIVACY TECHNOLOGY – A LANDSCAPE

Privacy Enhancing Technologies increased significantly to fix the privacy void by providing technological solutions that improve privacy in existing systems and practices. The PET solutions are both consumer-facing (demand-side) and business-facing (supply-side). On the supply side, PETs aid businesses in adhering to some of the fundamental principles of

[9] Shilpa Kumar et.al., Paving the Future: Why PrivacyTech is a rewarding frontier for venture capital, Omidyar Network India, Retrieved January 26, 2022 from https://www.omidyarnetwork.in/wp-content/uploads/ON-India-PrivacyTech-Thesis.pdf

[10] Venkatesh, Karthik and Shekar, Kamesh, Positive or Zero-Sum Game: When Privacy by Design Meets Dark Patterns (August 1, 2022). Available at SSRN: https://ssrn.com/abstract=4178549 or http://dx.doi.org/10.2139/ssrn.4178549

data protection like data minimisation, proactive data protection, end-to-end security and privacy-by-design, and in turn, aidding in compliance.[11] On the demand side, PETs are placed in a unique position where their consumer-facing solutions aid individuals in securing their data from privacy harm like financial loss[12], discriminatory treatment[13], exclusion[14], restrictions on free speech[15], and enhance user agency . Additionally, the Digital Personal Data Protection Bill 2022 provides consent managers who are meant to grant data principals increased autonomy over their data.

BOX 1
Privacy-enhancing Technology: Account Aggregator System

Similar to the Digital Personal Data Protection Bill 2022 Bill, NITI Aayog's draft Data Empowerment & Protection Architecture (DEPA) policy makes a case for a consent manager in the final layer of India Stack.

Following the draft DEPA policy, the Reserve Bank of India (RBI) notified the Master Direction for Non-Banking Financial Company - Account Aggregator in 2016. In September 2021, the Account Aggregator system was launched. Licensed under the category of NBFC, the Account Aggregator (NBFC-AA) will collect and share consumers' financial information with their consent from a financial information provider to a financial information user, acting as a consent manager for financial information transfer.

Besides, the technical aspects prescribed by RBI for NBFC-AA (NBFC - Account Aggregator (AA) API Specification, 2019) are mostly in line with the privacy by design principle.

The supply-side and demand-side PETs are tailored to fix the privacy void at different stages of the data lifecycle. While there are various PETs in the market, their implementation differs according to their maturity in technological readiness and solution quality[17]. The PETs discussed in this chapter are at the mid to complete maturity levels, where they are optimally ready for deployment. For example, end-to-end encryption is a

[11] Ruan, W., Xu, M., Jia, H., Wu, Z., Song, L., & Han, W. (2021). Privacy Compliance: Can Technology Come to the Rescue? Retrieved from IEEE Security & Privacy: https://www.computer.org/csdl/magazine/sp/2021/04/09444564/1u3mFH7L9gA

[12] Prasad, S. (2019, October 29). An Analysis of 'Harm' defined under the draft Personal Data Protection Bill, 2018. Retrieved January 17, 2022, from https://www.dvara.com/research/blog/2019/10/29/an-analysis-of-harm-defined-under-the-draft-personal-data-protection-bill-2018/

[13] Khan, L. M. (2017, January 3). Yale Law Journal - Amazon's Antitrust Paradox. The Yale Law Journal. Retrieved January 17, 2022, from https://www.yalelawjournal.org/note/amazons-antitrust-paradox

[14] A Taxonomy of Privacy - ORG Wiki. (2013, January 8). ORG Wiki. Retrieved January 17, 2022, from https://wiki.openrightsgroup.org/wiki/A_Taxonomy_of_Privacy#Exclusion;
Falling through the Cracks: Case Studies in Exclusion from Social Protection - Dvara Research. Retrieved January 17, 2022, from https://www.dvara.com/research/social-protection-initiative/falling-through-the-cracks-case-studies-in-exclusion-from-social-protection/

[15] Freedom of Expression & Privacy. (n.d.). The Centre for Internet and Society. Retrieved January 17, 2022, from https://cis-india.org/internet-governance/blog/freedom-of-expression-and-privacy.pdf

[16] Personal Data and Individual Agency. (n.d.). IEEE. https://ethicsinaction.ieee.org/wp-content/uploads/ead1e_personal_data.pdf

[17] Personal Data and Individual Agency. (n.d.). IEEE. https://ethicsinaction.ieee.org/wp-content/uploads/ead1e_personal_data.pdf

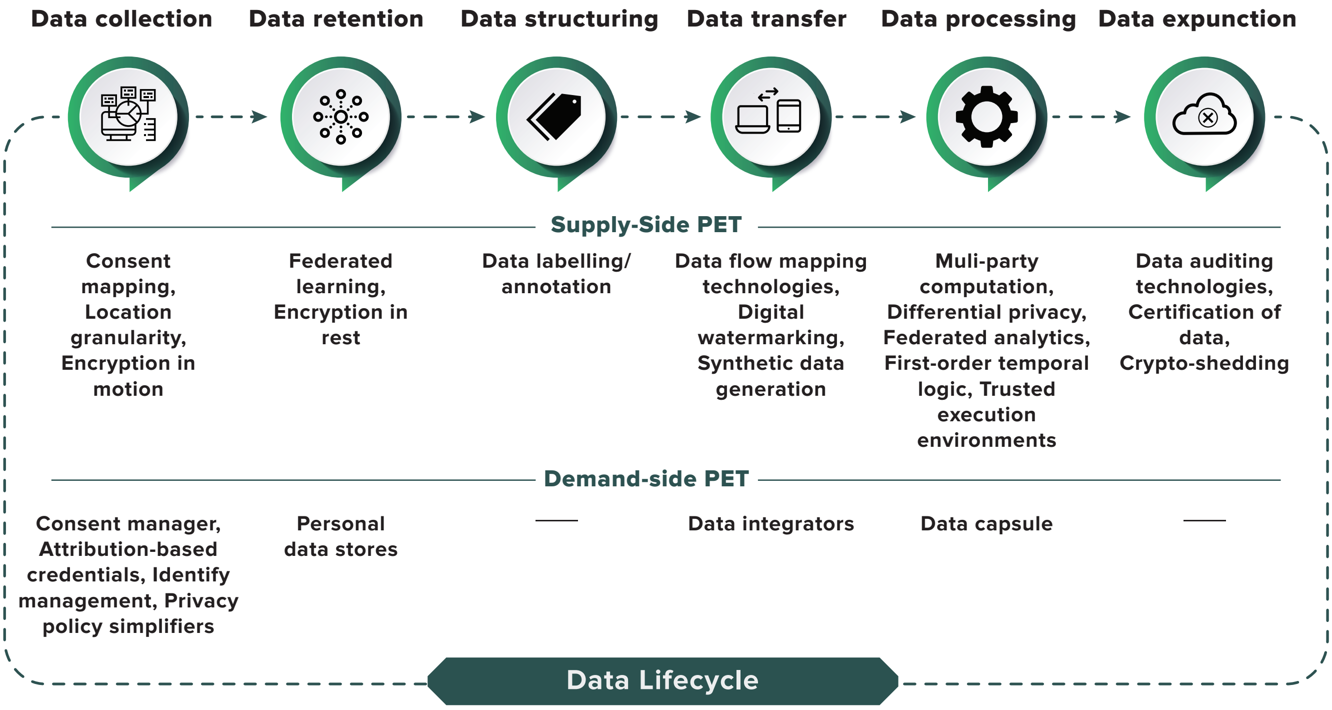
PET that is at a stage where deployment is possible at scale. However, homomorphic encryption, a kind of encryption technique that works differently from the E2EE and has different use cases, is still at the lab testing stage and is consequently not ready for deployment at scale. At the conclusion of this chapter, we discuss the journey of PETs to Privacy Preserving Technologies, which are novel technological solutions that guarantee user privacy.

3.1 MAPPING THE GROWTH OF PETS ACROSS THE DATA LIFECYCLE

Every data-driven industry and business has its functions, targets, and intended outcomes based on its specific business model and business requirements, but overarchingly they follow similar steps when dealing with data for extracting utility. While various pieces of literature[18] propose different classifications and models for understanding the data lifecycle, for the purpose of this chapter, we take the consensus of different classifications and divide the data lifecycle into six stages, i.e., data collection, data retention, data structuring, data transfer, data processing, and data expunction.

The classification is then used as a framework to categorise the available PETs across various stages of the data lifecycle. We study how each of these solutions and technology adds value to the company by easing compliance and promoting privacy outcomes.

Figure 6: Mapping PETs



	Data collection	Data retention	Data structuring	Data transfer	Data processing	Data expunction
Supply-Side PET	Consent mapping, Location granularity, Encryption in motion	Federated learning, Encryption in rest	Data labelling/ annotation	Data flow mapping technologies, Digital watermarking, Synthetic data generation	Muli-party computation, Differential privacy, Federated analytics, First-order temporal logic, Trusted execution environments	Data auditing technologies, Certification of data, Crypto-shedding
Demand-side PET	Consent manager, Attribution-based credentials, Identify management, Privacy policy simplifiers	Personal data stores	—	Data integrators	Data capsule	—

[18] Stobierski, T. (2021). 8 steps in the data life cycle. Retrieved from Harvard Business School: https://online.hbs.edu/blog/post/data-life-cycle;
Faroukhi, Z. (2020, January 8). Big data monetization throughout Big Data Value Chain: a comprehensive review - Journal of Big Data. Journal of Big Data. Retrieved January 17, 2022, from https://journalo¸igdata.springeropen. com/articles/10.1186/s40537-019-0281-5;
Curry, E. (2016). The Big Data Value Chain: Definitions, Concepts, and Theoretical Approaches. In New Horizons for a Data-Driven Economy (pp 29-37). https://link.springer.com/chapter/10.1007/978-3-319-21569-3_3;
For more literature on data value chain visit here.

3.1.1 Data collection

The first step that kickstarts the data lifecycle is data collection. An entity (data fiduciary) collects information about persons (data principal) in a variety of ways - both direct and indirect. Broadly, they can be grouped into the following –

(a) by directly seeking information from data principals, where individuals provide data in return for service;[19] and
(b) by indirectly through third parties, for instance, businesses approach data brokers (who aggregate data from multiple public sources[20]) to obtain data for marketing or authentication[21] purposes, among others.

While data collected through different means serve a particular purpose within the business operation of the data fiduciary, overall, at the point of the data collection stage, the data fiduciary is obliged to follow universal principles such as purpose limitation, data minimisation[22], and informed consent[23]. To aid business compliance with data minimisation mandates and to obtain informed consent for data collection, there are various supply-side (direct) and demand-side (indirect) PETs in the market, as discussed below.

Table 1: PETs - Data Collection

TECHNOLOGY	DESCRIPTION
Consent mapping[24]	It is a process for identifying data principals for seeking consent during data collection through third parties. There are solutions like consent mapping to simplify this process and make data fiduciaries compliant with consensual data collection. This technological solution maps data principals and automatically sends consent notices.
Location granularity[25]	They collect the location information of data principals and classify them based on granularity. Data principals can then avail of this service to disclose the granular amount of location data proportionate to the need for the same.

[19] Matsakis, L. (2019). The WIRED Guide to Your Personal Data (and Who Is Using It). Retrieved from WIRED: https://www.wired.com/story/wired-guide-personal-data-collection/

[20] Rafter, D. (2021). How data brokers find and sell your personal info. Retrieved from Norton: https://us.norton.com/internetsecurity-privacy-how-data-brokers-find-and-sell-your-personal-info.html

[21] Slater, A. (2014). The Costs and Benefits of Data Brokers. Retrieved from The Regulatory Review: https://www.theregreview.org/2014/06/19/19-slater-costs-and-benefits-of-data-brokers/

[22] The principles of data protection: not new and actually quite familiar. (2018, September 24). Privacy International. Retrieved January 17, 2022, from https://privacyinternational.org/news-analysis/2284/principles-data-protection-not-new-and-actually-quite-familiar

[23] Kosseim, P. (2017, May 15). Speech: Consent as a Universal Principle in Global Data Protection - May 15, 2017 - Office of the Privacy Commissioner of Canada. Office of the Privacy Commissioner of Canada. R etrieved January 17, 2022, from https://www.priv.gc.ca/en/opc-news/speeches/2017/sp-d_20170515_pk/

[24] Ruan, W., Xu, M., Jia, H., Wu, Z., Song, L., & Han, W. (2021). Privacy Compliance: Can Technology Come to the Rescue? Retrieved from IEEE Security & Privacy: https://www.computer.org/csdl/magazine/sp/2021/04/09444564/1u3mFH7L9gA

[25] Privacypatterns.org. (n.d.). Retrieved from https://www.privacypatterns.org/patterns/

Identity management	This privacy-enhancing solution helps data principals manage their multiple online identities and provide means to protect the data principals' primary identity by (a) access management solutions, i.e., controlling access to necessary information and (b) pseudonym management solutions, i.e., generating a proxy.[26] While this consumer-facing technology aids data principals to control the nature of data collection and to prevent their personal identity from being linked to data that they share, this solution also acts as a fixer between data principals and data fiduciaries by enabling privacy-secured transactions.
Consent manager	The consent manager acts as a conduit between the (a) data principal, (b) data fiduciaries who hold the data and (c) other data fiduciaries/processors to whom the data principal seeks to transfer the data. Consent managers aid data fiduciaries as the consent management for the data collection process is outsourced to them.
Attribute-based credentials[27]	Data fiduciaries collect data directly from data principals for authentication. Attribute-based credentials or ABC solutions minimise data at authentication, allowing for a highly flexible verification process. Using this solution, the data principals can choose to reveal only a relevant attribute of personal information for authentication thus aiding in complying with the data-minimisation principle. For instance, if age verification is mandatory for certain authentication, data principals can use ABC solutions to verify their age without disclosing their date of birth.
Privacy policy simplifiers	To reduce the fatigue[28] caused by reading the terms and conditions of various websites and services, this tool[29] scrapes the privacy policy of the website, simplifies it, and provides data principals with the information in an easily consumable format. This solution can reduce the compliance burden of data fiduciaries who are mandated to provide a simplified and consumable privacy policy for informed consent. In the Indian context, where regional differences create further challenges for obtaining informed consent, solutions with vernacular support can aid businesses in obtaining meaningful consent.

[26] Hansen, M., Berlich, P., Camenisch, J., & Clauß, S. (n.d.). Privacy-Enhancing Identity Management. 2004: Information Security Technical Report. Retrieved from Information Security Technical Report.

[27] Ruan, W., Xu, M., Jia, H., Wu, Z., Song, L., & Han, W. (2021). Privacy Compliance: Can Technology Come to the Rescue? Retrieved from IEEE Security & Privacy: https://www.computer.org/csdl/magazine/sp/2021/04/09444564/1u3mFH7L9gA

[28] Antithesis, some businesses provide readable privacy policies; for instance, the BBC's privacy policy scores high on the Lexile test due to short and plain language usage. Besides, Google and Apple provide consumer-friendly privacy policy interfaces, like short consent pop-ups before specific data collection for service.

[29] While this solution is still in the nascent stage, with informed consent increasingly becoming the bedrock of privacy regimes across the globe, there is scope for this solution.

Encryption in Motion	This tool enables data principals to secure the information from unauthorised access where data/information is converted into ciphertext, which only authorised recipients can decrypt with the key. This encryption-in-motion solution can aid data fiduciaries in preserving the privacy of the data principals and aligning with the data minimisation principle.

3.1.2 Data retention

Next in the pipeline, post collection and generation of the data is to retain it by storing it in the cloud servers or on physical devices, etc. The biggest threat that data fiduciaries face at the data storage stage relates to data breaches through hacking, leaks, etc. The impact of data breaches on an individual's right to privacy cannot be understated. They also have a negative knock-on effect on the reputation of data fiduciaries in addition to the costs of compensation. From a consumer perspective, data principals lose control over data at rest (when stored at the data fiduciaries' servers or with a third party), creating a lack of consumer choice and opacity in treating sensitive data like payments, medical history, etc. Restricting data retention practices is an important aspect of practising the principle of data minimisation and limitation. With these principles finding their way into the DPDPB, 2022 the following technologies can be used to go beyond merely fulfilling a legal obligation–such as proactive data protection,[30] user control of data,[31] etc.

Table 2: PETs - Data Retention

TECHNOLOGY	DESCRIPTION
Federated learning[32]	Federated learning is a solution that enables machine learning models to analyse decentralised data located in different local servers. This solution helps in decentralising data storage without compromising the business edge of processing data, thus reducing the risk of a data breach.
Encryption in Rest	This technological solution secures data stored on devices and servers, where the data on the server is converted into ciphertext that only authorised personnel with the encryption key can decode.

[30] GDPR – Article 25, 35

[31] GDPR – Chapter III; CCPA – Section 1 to 7; LGPD – Chapter III

[32] Bonawitz, K., Eichner, H., Grieskamp, W., Huba, D., Ingerman, A., Ivanov, V., Roselander, J. (2019). Towards Federated Learning at Scale: System Design. Retrieved from Cornell University: https://arxiv.org/pdf/1902.01046.pdf;
McMahan, B., & Ramage, D. (2017). Federated Learning: Collaborative Machine Learning without Centralized Training Data. Retrieved from Google AI Blog: https://ai.googleblog.com/2017/04/federated-learning-collaborative.html

Personal data stores (PDS)[33]	Using personal data stores, data principals can regain control over the stored data on the server through secure personal tokens. Various regulations globally including the upcoming DPDPB, 2022, vest data rights with users. This technological solution can aid data principals in exercising their rights and choice effectively by increased control over their data.

3.1.3 Data structuring

At the pre-processing stage, data fiduciaries train the data by sorting raw information, i.e., collected, generated and stored. The information of the data principal can be very loosely classified into personal, non-personal, sensitive, critical, and mixed data. Data fiduciaries also classify data and extract maximum value from it through precise predictions and usability. Usually, this classification is derived from legislation or policy.

Table 3: PETs - Data Structuring

TECHNOLOGY	DESCRIPTION
Data labelling/ annotation[34]	This solution aids data fiduciaries in cleaning, structuring and labelling data, which is the foundation for the machine learning tools used for processing. Labels allow the data fiduciaries to isolate variables within datasets and club them into buckets according to the nature and sensitivity of the data to stay privacy and data protection compliant. Data labelling solutions may also depend on machine learning models, which use various methods like synthetic labelling, programmatic labelling etc., for the annotation of data.

3.1.4 Data transfers

Data transfer is a process through which data fiduciaries exchange, port, and transmit data to a third party or other business entities. Data fiduciaries transfer data for business purposes like processing, research and development, marketing, etc. and for receiving data portability requests from data principals.

[33] Bolychevsky, I. (2018). Are Personal Data Stores about to become the NEXT BIG THING? Retrieved from https://medium.com/@shevski/are-personal-data-stores-about-to-become-the-next-big-thing-b767295ed842

[34] Polonetsky, J., & Greenberg, J. (2020). NSF Convergence Accelerator: The Future of Privacy Technology. Retrieved from Future of Privacy Forum: https://fpf.org/wp-content/uploads/2020/03/NSF_FPF-REPORT_C-Accel1939288_Public.pdf

This makes it difficult to trace the integrity of the data in terms of data provenance as identical data gets shared with different parties. But, the regulations push the data fiduciaries to map the data flow to assess privacy risks[35]. Therefore, data mapping is crucial for preserving privacy by assigning compliance to different actors during data transfers.

On the demand side, as data is scattered across various players, it is hard for the data principals to realise the actual value of data by transferring it from one entity to another. Solutions on the demand side trying to solve this problem by informing and allowing the data principal to access and integrate their personal data scattered across various players in a single dashboard.

Table 4: PETs - Data Transfers

TECHNOLOGY	DESCRIPTION
Data mapping solutions	There are various data mapping solutions in the market, which would aid data fiduciaries to trace the flow of data across various third parties, which increases the ease with which one can employ monitoring mechanisms across the lifecycle. These solutions also aid data fiduciaries in understanding the information lifecycle to identify unforeseen or unintended uses of the data.
Digital watermarking[36]	Using digital watermarking solutions, data fiduciaries can watermark the data while transferring it to third parties. This technology will place markers covertly on data to track and monitor the data transferred, protect data from anti-counterfeiting activities, etc.
Data integrators	Data integrators aid data aggregation efforts across multiple parties and enable the transfer of aggregated data to desired data fiduciaries. As data portability is right to be vested to data principals through various regulations globally, data integrators can aid data fiduciaries in enabling portability in privacy preserved fashion.

3.1.5 Data processing

One of the significant stages of the data lifecycle is the data processing phase, where data fiduciaries process data for a multitude of services, including but not limited to marketing, improved service delivery, securing competitive advantages etc. Insufficient adherence to the principles of purpose limitation, data minimisation and privacy violations also make the

[35] For instance, Article 30 of GDPR mandates data flow mapping.

[36] L.Ou, Z.Qin, H.Yin, & K.Li. (2016). Security and Privacy in Big Data. In R. Buyya, R. N. Calheiros, & A. V. Dastjerdi, Big Data: Principles and Paradigms.

data more vulnerable to cybersecurity breaches both at input and output levels. From the demand-side, data principals are unaware of how their data is processed, thus losing control over it. To weed out these inconsistencies, there are various business-facing and consumer-facing PETs in the market.

Table 5: PETs - Data Processing

TECHNOLOGY	DESCRIPTION
Multi-party computation (MPC)[37]	This solution branches out from cryptography, where different untrusted players process data through private distributed computations. This computation allows different players to analyse data without revealing their private input. Therefore, this solution aims for a positive-sum game where privacy is kept intact while processing the data for extracting utility.
Differential privacy	At the output level, a differential privacy solution helps to share aggregate information of data principals while preserving privacy. This solution also keeps the probability of identifying the data principal low. Differential privacy forms data anonymity via injecting noise into the dataset. It allows data fiduciaries to execute all possible (functional) statistical analyses without identifying personal information.
First-order temporal logic	This solution provides automatic system monitoring/ oversight on the processing of data in line with data processing restrictions imposed by regulations and users. Using this solution data fiduciaries can monitor their processing activities to avoid regulatory breaches.
Trusted execution environments (TEE)[38]	TEE is commonly known as an isolated processing environment in which applications can be securely executed irrespective of the rest of the system. This solution creates a secured environment within the main server where the operating system cannot read the code within the TEE. Therefore, this solution aids data fiduciaries in maintaining confidentiality and integrity of data while processing.

[37] Dilmegani, C. (2020). Top 10 Privacy Enhancing Technologies (PETs) & Use Cases. Retrieved from AI Multiple: https://research.aimultiple.com/privacy-enhancing-technologies/

[38] Ruan, W., Xu, M., Jia, H., Wu, Z., Song, L., & Han, W. (2021). Privacy Compliance: Can Technology Come to the Rescue? Retrieved from IEEE Security & Privacy: https://www.computer.org/csdl/magazine/sp/2021/04/09444564/1u3mFH7L9gA

Data capsule[39]	This consumer-facing solution aids data principals in manually creating policies in accordance with which their data can be processed. Data principals can also develop purpose-specific policies with data capsules. This solution will aid data fiduciaries to be aware of the sensitivity of the data according to data principals' preferences during processing.

3.1.6 Data expunction

The final stage in the data lifecycle is deleting the data once it has served its purpose or on the insistence of the data principal, whichever is earlier. India has provided for the right to erasure in the latest DPDPB, 2022.[40] These regulations also empower data principals to seek deletion or correction of data (through consent withdrawal) if they think it no longer serves the purpose.

Table 6: PETs - Data Expunction

TECHNOLOGY	DESCRIPTION
Data auditing technologies	These help expunge unnecessary data collected throughout the lifecycle. Audit functions can also help fiduciaries identify new ways of using their data (raw or the database created).
Certification of data destruction	This solution provides an audit document that certifies data fiduciaries to have undergone the data destruction process. This document acts as proof of data fiduciaries' compliance with data protection regulations and enhances transparency.

It is clear that privacy-enhancing technologies are moving in a positive trajectory. While there is a significant development in PETs at stages like data processing and data transfers; there is tremendous scope for improvement in stages like data expunction, data training, etc.

[39] Wang, L., Near, J. P., Somani, N., Gao, P., Low, A., Dao, D., & Song, D. (2019). Data Capsule: A New Paradigm for Automatic Compliance with Data Privacy Regulations. Retrieved from Cornell University: https://arxiv.org/abs/1909.00077

[40] Clause 39

3.2 EVOLUTION OF PRIVACY PRESERVING TECHNOLOGY

Privacy technology in India, as an industry, is still in its nascent stages. Considering the staggered adoption of data protection regulations across the globe, the privacy technology industry has also developed at a relatively slow pace. As discussed earlier, the larger problem is the absence of a privacy culture within businesses and on the consumer side.

Another reason for the slow uptake of privacy technology in India and across the globe is the absence of standardised privacy terminology.[41] There are no uniform industry standards to conduct risk assessments or develop standardised technology that can be effectively used globally. For example, a privacy technology can have various use cases, each with distinct levels of effectiveness. The result of such fragmentation is that there are several classifications of privacy technology. The ambiguity has thus created a disjointed privacy technology industry. Therefore, while businesses are making decisions regarding the onboarding of privacy technology solutions, they must take into consideration the Technology Readiness Level of the privacy solution they choose to adopt.[42] ENISA, the EU Agency for Cybersecurity, has developed an assessment methodology for determining the readiness of privacy-tech solutions.[43] Conducting such an assessment will also introduce a degree of harmony within the industry as available solutions, and their shortcomings will be made clear.[44]

Another classification adopted by a few is that of ‘privacy-preserving technology’ and ‘privacy enhancing technology’. PETs are said to have evolved in the first phase of the privacy technology industry in the West, marked by the enactment of the General Data Protection Regulation in the European Union or the California Consumer Privacy Act, 2018. Privacy Enhancing Technology would, therefore, have preceded the use of Privacy Preserving Technology.[45] The significant penalties imposed by data protection regulation in case of non-compliance encouraged several business entities to adopt privacy technology that was focused on simplifying the compliance processes of businesses. The goal, therefore, was to adopt technology that allowed one to maximize or enhance privacy in existing systems and processes. These technologies are therefore dubbed ‘Privacy Enhancing Technologies’.

However, with the evolution of privacy and the beginnings of a privacy culture in the West, several business entities wished to develop a privacy-first approach. The privacy-by-design principles[46], while introduced in the 1990s, began slowly translating into technological solutions. Privacy-Preserving Technologies are those that developed novel solutions or technologies to address a specific concern, commonly beyond mere compliance solutions.

[41] Privacy Tech Alliance & Future of Privacy Forum, Privacy Tech’s Third Generation, FPF (June. 2021), https://fpf.org/wp-content/uploads/2021/06/FPF-PTA-Report_Digital.pdf

[42] Ibid

[43] Ibid

[44] Ibid

[45] Ibid

[46] Ann Cavoukian, Privacy by Design: The 7 Foundational Principles, 2009, https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf

These are technologies which guarantee privacy to an individual, while PETs simply improve privacy in existing systems.[47] The goal of privacy-tech vendors has evolved to provide solutions that maximise the value of data throughout the business.[48] These technologies span across the following key areas:

1. Making personal data accessible/available for marketing/unlocking the value of data.[49] These would include technologies like Secure Multi-Party Computation, homomorphic encryption, differential privacy, etc.
2. Increasing end-user control and engaging in user-centric data protection practices.[50] These include consent mapping, consent managers, etc.
3. Developing solutions for automated compliance and tools for transparency.[51] These include technologies based on Fully Homomorphic Encryption principles, data disruption exchanges, Trusted Execution Environments, etc.

It is clear, therefore, that to successfully meet all their data needs, a business will have to layer several integrated solutions. Developing such technology and creating a homogenous market will be even more challenging in the future because the privacy landscape will become more complex, with various jurisdictions diverging in their regulatory approaches. Most companies, however, do not have the resources and expertise required to build these technologies in-house. They, therefore, have to rely on privacy technology vendors to be able to provide the solutions. The next chapter will delve into the challenges associated with adopting privacy technology in greater detail.

4 STRUCTURAL CHALLENGES FOR PRIVACY TECHNOLOGY

4.1 THE TREND OF LEGAL ENDOGENEITY

Leading scholars has traced the evolution of privacy law from its traditional notice-and-consent mechanisms to include a combination of individual rights of control and internal compliance structures. Laura Edelman posits that any law, over time, shows a trend in its compliance wherein the overall culture of the form of law starts taking

[47] Data Protection in the Era of Artificial Intelligence, Big Data Value Association, (Oct. 2019), https://www.bdva.eu/sites/default/files/Data%20protection%20in%20the%20era%20of%20big%20data%20for%20artificial%20intelligence_BDVA_FINAL.pdf

[48] Privacy Tech Alliance & Future of Privacy Forum, Privacy Tech's Third Generation, FPF (June. 2021), https://fpf.org/wp-content/uploads/2021/06/FPF-PTA-Report_Digital.pdf

[49] Ibid

[50] Data Protection in the Era of Artificial Intelligence, Big Data Value Association, (Oct. 2019), https://www.bdva.eu/sites/default/files/Data%20protection%20in%20the%20era%20of%20big%20data%20for%20artificial%20intelligence_BDVA_FINAL.pdf

[51] Ibid

precedence over its substance – a process termed as 'legal endogeneity'.[52] Privacy laws and technology in India face this structural challenge, not unique to a national context, to its implementation and desired outcomes.

Edelman studied the phenomenon of legal endogeneity in the American context of enforcement of civil rights in workplaces. She describes how developing an anti-discrimination policy is a necessary first step in creating an inclusive working environment, but it becomes a mere symbolic structure until actively enforced. However, these symbolic structures have increasingly gained the legitimate status of 'law' itself.[53] In other words, the act of developing an internal complaints process or appointing a diversity officer is looked at as complying with the law. These actions would hardly lose their legitimacy even if they were to grant the aforementioned diversity officer no powers or overturn every complaint in the review process.[54]

As described by Edelman, there are several stages through which a culture of legal endogeneity can be observed. It begins with the enactment of legislation that has ambiguity in application. The absence of clarity in law gives practitioners on the ground the leeway to interpret and implement the law in a manner that benefits them.[55] Left to their own devices, practitioners often recast their obligations from the substance (such as preventing discrimination, for instance) to procedure (such as drafting an anti-discrimination policy).

A. E. Waldman, a celebrated privacy scholar, describes the matter of legal endogeneity in the context of privacy laws in the United States. He claims that the overwhelming complexity and dynamic nature of privacy laws have created a significant degree of ambiguity. For example, the Federal Trade Commission in the United States requires that individuals are given 'adequate' notice by companies regarding the use of their personal data.[56] However, the term adequate remains undefined. This results in several hard-to-read privacy policies that are hardly ever read by consumers. Even so, the existence of a privacy policy became a proxy signifying the enforcement of privacy law to courts and regulators. Privacy law, unlike civil rights law, is dominated by a technology market. The novelty of the new-age technology and the scale at which the market grows accelerates the trend of judicial bodies deferring to the expertise of industry professionals. Judicial bodies are sometimes of the opinion that they do not have the requisite knowledge to answer questions of privacy law because it is steeped in technology.[57]

4.2 LIMITS OF TECHNOLOGICAL OUTSOURCING

The overall tendency of endogeneity, therefore, can be identified in privacy technology that codifies the interpretations of privacy law in their system design. These interpretations are rarely if ever, made by privacy or legal professionals but rather in the field of privacy

[52] Ari Ezra Waldman, Privacy Law's False Promise, WASH. U. L. REV. 0773 (2020).
[53] Ibid.
[54] Ibid.
[55] Ibid.
[56] Ibid.
[57] Ibid.

engineering.[58] While the privacy technology sector is relatively new, the existing practices will eventually shape the law itself. Makers of technology, because of market pressures, may be more concerned with whether or not a law can be easily articulated in system design rather than focusing on the substantive goal of securing privacy outcomes of individuals or communities.

In his paper titled Outsourcing Privacy, Waldman discusses how systemic outsourcing in the privacy space in the United States has had a widespread effect on privacy as a culture. He describes the rise of a framework that calls for institutions to be organised around the values of efficiency, productivity and innovation.' The primary argument he makes is that the manner in which privacy compliance practices have evolved, such as the practice of outsourcing compliance operations to privacy-tech vendors, has led to a minimal focus on substantive adherence to the goals of privacy law and more on reducing bottlenecks for product innovation.

The privacy regulatory landscape is only becoming more complex as more jurisdictions develop their data protection laws. Interpreting the laws themselves is challenging for privacy law experts and others in the judicial field. Privacy technology vendors and anyone that is meant to comply with privacy law must first understand the regulation and its requirements. However, the development of privacy technology often occurs with little to no legal expertise on the team. When privacy technology vendors develop such 'solutions', they do so, keeping the corporate goals of efficiency, productivity, and innovation. Their interpretation of privacy law in itself is skewed. The goal is not that of securing the data of the end-user but to comply with regulation while engaging in unabated data-extractive practices behind the scenes.

Without specific laws or organisational policies, privacy technology vendors end up codifying their own definitions and interpretations of privacy laws into the technology they build.[59] A few technologies that do this include a compliance technology which claims that it is 'GDPR Ready' and helps organisations attain, maintain and demonstrate ongoing compliance.[60] Another vendor that provides privacy and security solutions to healthcare providers and guarantees compliance with Article 25 of the GDPR and fully addresses five of the Phase 2 HIPAA[61] Audit protocol elements and 'partially addresses' twenty-six more.[62]

Waldman conclusively states that this approach has reduced the effectiveness of privacy regulation by converting policies, privacy impact assessments and audit frameworks to symbolic measures. He argues that a company only outsources functions and responsibilities that are not part of its core competencies.[63] When a company outsources privacy-related tasks, they do so perhaps because it is not their core expertise, but that does not mean competencies should not be built up over time. This trend is particularly worrisome when the company collects, stores and processes vast amounts of data. Such systemic outsourcing can lead to the following issues:

[58] A.E.Waldman, Outsourcing Privacy, 96 Notre Dame L. Rev. Reflection 194 (2021)

[59] Ibid

[60] Antonenko, D. (2022, April 9). GDPR Compliance Technology. Businesstechweekly.com. Retrieved October 20, 2022, from https://www.businesstechweekly.com/legal-and-compliance/gdpr-legislation/gdpr-compliance-technology/

[61] HIPAA is an American legislation enacted to develop and enforce standards of healthcare, specifically data collection and sharing practices, across the country.

[62] A.E.Waldman, Outsourcing Privacy, 96 Notre Dame L. Rev. Reflection 194 (2021)

[63] Ibid

4.2.1 Power Asymmetries

Developing an in-house capacity of privacy solutions requires the following – firstly, resources to set up in-house technical experience, accommodate large salaries, benefits for new employees and create institutional time and capacity; secondly, legwork which allows a company to develop a clear set of goals, ongoing relationship maintenance, technological assessment, employee training etc.

It is clear that larger companies are better positioned, therefore, to develop their in-house privacy capacity, while smaller entities that are strapped for time and resources cannot afford to do so. This inevitably gives the larger entities a competitive advantage as they are able to adhere to privacy regulations and advertise the same to their consumers. Several companies in Singapore have also begun advertising their updated privacy policies to highlight their commitment to protecting individual data.[64]

4.2.2 Narrowing Privacy Law

Waldman argues that to operationalise privacy outcomes, as a first step, one must consider managing users' expectations, their desire for obscurity, and their need for trust. In their interpretation of privacy law, however, vendors reduce the law to modifiable factors that can be easily identified by Artificial Intelligence (AI). It also shifts focus from the larger objective of reducing privacy risks for consumers to reducing litigation risks for the business. This has created a culture where laws are drafted with this managerial objective in mind. Laws are, therefore, limited to easily codifiable provisions in system designs.[65]

4.2.3 Erosion of Expertise

As discussed earlier, technology vendors rarely employ legal experts to be part of their teams. People with no legal experience end up burying their conclusions into code, which inevitably creates a product of poorer quality. Waldman also discusses this concept in his paper titled 'Privacy Law's False Promise'. Here, he points out that while involving in-house attorneys and privacy professionals in the design process of privacy-tech is ideal, it is also expensive. Limiting the scope of activity of PET vendors to something like information management is also unrealistic.

4.2.4 Lack of Accountability

The introduction of privacy-safe techniques takes place in the design process of such technologies. Waldman argues that the design process is also when privacy laws are instantiated. Those in due diligence teams, such as audit teams, are often shielded from this design process. In his book, 'Industry Unbound', Waldman discusses his experience with several companies' in-house privacy experts. The expert is often assigned to a

[64] Claudia Lim, Singapore's Reationship to Data Privacy May be Evolving, Iris, (1 June 2021), from https://participationindex.iris-worldwide.com/2021/06/01/singapores-relationship-with-data-privacy-may-be-evolving/

[65] A.E.Waldman, Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power, Cambridge University Press (28 Sept., 2021).

product or engineering team. However, the reporting requirements within the corporate structure often require the engineer to spot the privacy issue and report it to his manager. The issue then travels up the corporate ladder and often reaches the privacy expert only at a late stage of the design process.[66]

5 OPERATIONAL CHALLENGES FOR PRIVACY TECHNOLOGY

The Indian industry has developed privacy-tech solutions that are arguably sufficiently mature to meet the compliance needs of businesses today. PETs that can enhance privacy at each data lifecycle stage through various functions like consent mapping, data labelling and encryption are available for enterprise use. Further, PPTs or novel systems and solutions that preserve the privacy of user data, have also seen notable growth. However, certain operational bottlenecks have held back the adoption of privacy technology. In this chapter, we will analyse operational challenges in the following groupings:

1. Demand side challenges limiting the uptake of privacy-tech by businesses
2. Supply side challenges preventing the growth of privacy-tech solutions

5.1 DEMAND-SIDE CHALLENGES

Policymakers are stressing on the significance of data privacy in the light of rising data breaches at various companies. Additionally, the expectations of users from companies to protect their data is rising. According to a recent survey of 6000 Indian respondents, 84% of consumers surveyed prefer organisations that are committed to protecting their privacy.[67] In light of these trends, privacy-tech vendors anticipate the rising adoption of their solutions. According to our review, there are six major challenges currently holding back businesses from adopting privacy-tech solutions.

5.1.1 Lack of a privacy-centric culture

Businesses primarily look at privacy protection to – first, ensure compliance with data protection laws and consequently reduce legal risks, and secondly, to prevent data breaches in order to prevent reputational and financial damage.[68] These are genuine concerns, considering that penalties for non-violation of laws, combined with litigation

[66] A.E.Waldman, How Big Tech Turn Sprivacy Law Into Privacy Theatre, Slate, Retrieved on January 2, 2021 from https://slate.com/technology/2021/12/facebook-twitter-big-tech-privacy-sham.html.

[67] Hemai Sheth, (2021, March 14), 84% Indian consumers willing to pay more to do business with organisations committed to protecting data privacy: Report, The Hindu Business Line, Retrieved February 16, 2022 from https://www.thehindubusinessline.com/info-tech/84-indian-consumers-willing-to-pay-more-to-do-business-with-organisations-committed-to-protecting-data-privacy-report/article34066225.ece

[68] Data Privacy study: 500 companies share their insights, (2020, May 22), Data Privacy Manager, Retrieved February 16, 2022 from https://dataprivacymanager.net/data-privacy-study-500-companies-share-their-insights/; How Organizations are Managing Cyber Risk in a Fast-Changing Business Environment: Marsh Microsoft 2019 Cyber Survey Results, (2019, October 7), MARSH, https://www.marsh.com/content/dam/marsh/Documents/PDF/US-en/marsh-microsoft-cyber-survey-report-2019-webcast-slide.pdf at 11; IAPP 2021 Tech Vendor Report, (2021), IAPP, https://iapp.org/media/pdf/resource_center/2021TechVendorReport.pdf at 35.

costs, can be significant. At the same time, costs of data breach have reached record highs during the pandemic. The 2021 Cost of a Data Breach Report from IBM security revealed that in India, Rs. 5,900 was the cost to the company per lost or stolen record in 2021.[69] The average total cost of a data breach was the highest in the healthcare and financial sector.[70] According to the survey, anonymised customer data was the second most common type of record compromised, preceded by customer personal identifiable information (PII was the most common type.[71] The report considers hundreds of cost factors involved in data breach incidents, including loss of customers and brand equity.

As a result, businesses are relying more on lawyers to ensure regulatory compliance and cybersecurity solutions to prevent data leaks. With the enactment of the DPDPB 2022, it is likely that this dependency will only increase. While resolving these concerns is integral to business operations, the culture does not allow for proportionate attention to the data privacy interests of the users. One of the reasons behind this is that privacy is often understood from risk perspectives – as focused on managing corporate risk, balancing regulation and profit and enhancing innovation. The effect of this is often the frustration of consumer privacy rights.[72] The DPDPB, 2022, for instance, provides for the right to correct and erasure consent mechanisms, while the digital health sector in India has already envisaged the application of consent managers to access longitudinal records.[73] These priorities are often also reflected in national policies pertaining to technology. For instance, public engagement values and mechanisms are rarely salient in consolidating AI regimes. Therefore, they do not always prioritise protecting the interests of the users.[74] Absence of governing policies that do not prioritise user interest can influence organisational cultures and values in the private sector.

There exists a need for businesses to move towards a privacy-centric culture that prioritises the protection of user privacy while also looking after concerns of non-compliance and data leaks. For instance, a focus on efficiently recording user consent through consent management solutions can considerably enhance the autonomy of users over their data. At the same time, this approach can i assist in adhering to legal requirements that mandate processing of data only according to purposes consented to and ii reduce risks associated with data leakage by ensuring that data is shared strictly in accordance with user consent.

The issue of insufficient attention is not limited to the protection of user privacy. The challenge also extends to responsible value creation from data. Over time, businesses have witnessed an increase in the influx of data. However, they continue to be overwhelmed by it and are not deriving sufficient value from it. This has also played a role in slowing down the adoption of privacy-tech solutions, as we will see in the next section.

[69] PTI, (2021, July 28), Cost of data breach hits record high during pandemic: IBM, Financial Express Retrieved February 16, 2022 from https://www.financialexpress.com/industry/cost-of-data-breach-hits-record-high-during-pandemic-ibm/2299709/.

[70] Cost of a data breach report 2021, (2021, July), IBM, Retrieved February 16, 2022 from https://www.ibm.com/downloads/cas/OJDVQGRY at 15.

[71] Cost of a data breach report 2021, (2021, July), IBM, Retrieved February 16, 2022 from https://www.ibm.com/downloads/cas/OJDVQGRY at 15.

[72] Waldman, A., Privacy Law's False Promise (2019, December 6). Washington University Law Review, Vol. 97, No. 2, 2020, Retrieved February 16, 2022 from SSRN: https://ssrn.com/abstract=3499913 at 49.

[73] Ministry of Health and Family Welfare, National Digital Health Blueprint (30 Jan. 2020), from https://main.mohfw.gov.in/sites/default/files/Final%20NDHB%20report_0.pdf.

[74] Wilson, C., (2022, January), Public engagement and AI: A values analysis of national strategies, Government Information Quarterly Vol 39 Issue No. 1, Retrieved February 16, 2022 from https://doi.org/10.1016/j.giq.2021.101652

5.1.2 Limited focus on creating value out of data

In addition to protecting user privacy, privacy-tech solutions can enable processes that can assist in responsibly deriving value out of data.[75] This can be achieved in two ways. Firstly, privacy-tech can enable processes beneficial for value derivation from data. For instance, technologies like data mapping solutions can provide businesses with an insight into how data moves through their systems, including the identity of data collected, sources of ingestion, purpose, retention timelines, and access controls. Therefore, it can ensure that data in various silos do not go undetected and can inform business decisions. Secondly, privacy-tech solutions can balance data utility with the privacy of data, thereby enabling long-term sustainable data processing activities that do not have any regulatory risk. For instance, homomorphic encryption can enable computations on encrypted data without first decrypting it, serving as a sustainable mode of privacy-centric value creation. Businesses that safely and consistently derive value from data would, therefore, recognise the value of privacy technology.

According to a cross-jurisdictional study by Forrester[76] of 45 locations including India, the United States, and various European countries, 70% of data decision-makers are gathering data faster than they can analyse and use it and most (88% of them are neglecting either the technology and processes or culture and skills or both required for creating value out of data. This has led to businesses being unable to analyse and derive value out of most data collected by them. A report by Deloitte highlights that Indian companies often do not use more than 5-20% of the personal data they collect.[77] Increased focus on creating value out of data which entails identifying use-cases of data insights, implementing internal processes for analysing insights and incorporating appropriate solutions can help businesses innovate and customise services to consumer needs. Additionally, it can foster increased adoption of privacy-tech solutions.

The willingness of businesses to invest in privacy-tech solutions is not only influenced by demand from users. The extent of awareness among businesses about incentives that can be derived out of these solutions can also determine whether companies would be keen to invest in privacy-tech solutions or not is also a relevant point here.

[75] Timan T., (2019, October), Data Protection In The Era Of Artificial Intelligence, BDVA Retrieved February 16, 2022 from https://www.bdva.eu/sites/default/files/Data%20protection%20in%20the%20era%20of%20big%20data%20for%20artificial%20intelligence_BDVA_FINAL.pdf at 16;
Protecting Privacy in practice, (2019, March), The Royal Society, Retrieved February 16, 2022 from https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/privacy-enhancing-technologies-report.pdf at 26. at pg. 26

[76] Unveiling Data Challenges Affecting Businesses Around The World. (n.d.). Dell. Retrieved October 20, 2022, from https://www.delltechnologies.com/asset/en-in/solutions/industry-solutions/industry-market/data-paradox-forrester-thought-leadership-paper.pdf

[77] Rajendran V. & Sehgal M., (2019), Unlocking the Potential of India's Digital Economy : Practices, Privacy and Governance, Omidyar Network India And Deloitte, Retrieved February 16, 2022 from https://www2.deloitte.com/content/dam/Deloitte/in/Documents/about-deloitte/Privacy_and_Data_Ethics-A_Roadmap_for_India_Report_V4.pdf.

5.1.3 Low demand from users

With the backdrop of rising privacy breaches and discourse on data protection laws, the relevance of privacy protection has increased for consumers as they are now more aware of their data rights.[78] This is down to focused efforts from various stakeholders. For instance, civil society is publishing literature that raises awareness of privacy rights. Companies are leveraging their privacy protection capacities as a competitive differentiator to attract consumers.

However, there is a long way to go before privacy concerns of users can significantly impact their behaviour while using technology, including their decision to use or not use certain services. Concerns about privacy are not yet driving consumer behaviour, despite rising awareness; as their online activity is only increasing.[79] Further; consumers are regularly trading their privacy rights for benefits provided by technology. This phenomenon has been termed as the 'privacy paradox'.[80] Recent research has revealed that while users are concerned about their privacy, they nevertheless undertake very little action to protect their personal data.[81] Difficulty in understanding the manner in which their data is processed and cumbersome processes for managing privacy are a few reasons behind this. To this end, consumers often find it easier to be apathetic to privacy concerns while making purchasing decisions. An increase in consumer demand for effective privacy protection practices can potentially incentivise businesses to adopt privacy-tech solutions.

5.1.4 Limited awareness of business incentives

While businesses are aware of the disincentives of not implementing privacy-protecting practices, positive incentives like investor appeal and prospects of international expansion are yet to be realised. Hefty penalties under data protection laws disincentivise inefficient data protection practices by businesses. For instance, The Privacy Legislation Amendment (Enforcement and Other Measures Bill 2022 provides for a fine of AUD 500 million or 30% of a company's adjustment turnover, whichever is greater, for the breach of the law.[82] The recent iteration of India's data protection regulations has also indicated that financial penalties will be borne by data fiduciaries in cases of violation.[83] This represents an overall shift towards imposing mandatory data protection practices across various industries. However, in order to ensure meaningful compliance through privacy-tech solutions,

[78] Has Lockdown made Consumers more open to Privacy? (2020), EY Global Consumer Privacy Study 2020 Retrieved February 16, 2022 from https://assets.ey.com/content/dam/ey-sites/ey-com/es_es/topics/resilient-enterprise/ey-global-consumer-privacy-study-2020-single-pages.pdf.

[79] Lee, P. et.al., (2021, December 8), Are data privacy concerns driving consumer behavior? Not yet., Deloitte, Retrieved February 16, 2022 from https://www2.deloitte.com/us/en/insights/industry/technology/protecting-consumer-data.html

[80] Brown, B. (2001), Studying the internet experience, Hewlett Packard, Retrieved February 16, 2022 from https://www.hpl.hp.com/techreports/2001/HPL-2001-49.pdf

[81] Barth, S. & Menno D (2017), The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review, 34(7) Telematics and Informatics 1038, Retrieved February 16, 2022 https://www.sciencedirect.com/science/article/pii/S0736585317302022.

[82] Cl. 14, Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 from https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6940.
https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6940.

[83] Cl. 25, Ministry of Electronics and Information Technology, The Digital Personal Data Protection Bill, 2022, from https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Protection%20Bill%2C%202022.pdf.

businesses need to realise positive incentives of privacy protection as well. A global study by Cisco highlighted that only 36% of the surveyed businesses recognised investor appeal as a business benefit of privacy investment.[84]

In addition to investor appeal, privacy- tech solutions can enhance future business prospects by preparing it for expansion into jurisdictions with strict data protection laws. Regulatory frameworks have the potential to create entry barriers in certain markets, as has been acknowledged by antitrust frameworks of various jurisdictions.[85] Data privacy laws, without effective preparation and funding, can make it difficult for companies processing data to operate feasibly in the concerned jurisdiction.[86] Therefore, incorporating privacy- tech solutions can assist companies in overcoming regulatory barriers and effectively competing in jurisdictions with strict data privacy regimes. Consequently, these factors can impact a business's valuation while raising funds. Continued oblivion to these factors can affect their willingness to adopt privacy-tech and slow their growth. Limited awareness of business incentives can influence budgetary decisions pertaining to privacy- tech solutions, further stalling the adoption of these services.

5.1.5 Budgetary restrictions

Lack of resources for the protection of privacy has also held back the adoption of privacy-tech.[87] There are multiple reasons for the budgetary restrictions. First, since businesses have not sufficiently realised the financial benefits of integrating privacy-tech, budget allocations for these solutions remain limited. In the short-term, privacy-tech investments can be challenging and cost-intensive for enterprises with limited resources as they may require a notable investment of funds, time, and human resources. However, in the longer term, financial incentives for investment in privacy-tech show up, which can justify the budgetary allocations. These benefits include shorter sales delays due to customer data privacy concerns as well as shorter system downtimes during a data breach.[88]

Secondly, the budget for various privacy-tech solutions would be determined by an entirely new budget head[89] that can only be accommodated with sufficient time and analysis of

[84] White Paper on Privacy Gains: Business Benefits of Privacy Investment, Cisco (2019), Retrieved February 16, 2022 from https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/privacy-gains-business-benefits-of-privacy-investment-white-paper.pdf.

[85] Competition and barriers to entry, (2007, January), OECD, Retrieved February 16, 2022 from https://www.oecd.org/competition/mergers/37921908.pdf.

[86] Kerber, W. & Specht-Riemenschneider, L., (2020, September 30), Synergies Between Data Protection Law And Competition Law, VZBV Retrieved February 16, 2022 from https://www.vzbv.de/sites/default/files/2021-11/21-11-10_Kerber_Specht-Riemenschneider_Study_Synergies_Betwen_Data%20protection_and_Competition_Law.pdf

[87] How Privacy Tech Is Bought and Deployed, (2019), IAPP & TrustArc, Retrieved February 16, 2022 from https://iapp.org/media/pdf/resource_center/privacy_tech_bought_and_deployed_IAPPTrustArc_2019.pdf..

[88] White Paper on Privacy Gains: Business Benefits of Privacy Investment, Cisco (2019), Retrieved February 16, 2022 from https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/privacy-gains-business-benefits-of-privacy-investment-white-paper.pdf at 3.

[89] Kumar, S. et.al., (2021), Paving the Future: Why PrivacyTech is a rewarding frontier for venture capital, Omidyar Network India, Retrieved February 16, 2022 from https://www.omidyarnetwork.in/wp-content/uploads/Privacy-Tech-Thesis-July7.pdf.

returns. Thirdly, while IT professionals may understand the nuanced benefits of privacy- tech solutions, but those with authority over the allocation of budgets may not. Streamlining operational processes and stakeholder interaction on budget decisions can, thus, facilitate investment in privacy-tech solutions.

In addition to budgetary restrictions, there are other factors as well that impact the ability of a business to adopt privacy-tech solutions. Most importantly, these include gaps in knowledge and internal processes that concern the adoption of privacy-tech.

5.1.6 Gap in knowledge and internal processes

Businesses with the intent to adopt privacy- tech often have limited awareness of state-of-the-art technologies. In cases where companies are aware of the latest technologies, they are either unclear about which use cases can benefit from them or have the impression that easy-to-use solutions are unavailable.[90]

Further, organisations are unable to adopt privacy technology due to a gap in internal processes. Businesses often do not have dedicated roles to manage conflicts arising out of product and engineering decisions on user privacy.[91] Absence of institutionalised process workflows and standard operating procedures on data privacy, limits their ability to integrate privacy-tech in their operations.[92] Understanding the relevance, use cases and integration strategies of privacy-tech is crucial to adopt these technologies.

To ensure that the uptake of privacy-tech increases among businesses, it is crucial that bottlenecks pertaining to culture, demand, knowledge, internal processes, and budgets are sufficiently studied.

5.2 SUPPLY-SIDE CHALLENGES

Out of 365 privacy-tech vendors identified in the IAPP 2021 Tech Vendor Report, only 7 are from India. These companies provide a range of services, including data mapping, identification/pseudonymity, and consent management solutions. These solutions assist in various stages of the data lifecycle by efficiently mapping the processing journey of data, anonymising sensitive data and ensuring adherence to the consent provided by data principals. Currently, market studies on the privacy-tech sector in India are scarce.

Certain trends specific to the Indian context are worth mentioning. First, a notable number of vendors[93] in the country provide a multitude of services to businesses, rather than hyper-specialising in a particular technology. Assessment managers and services that can optimise data processing like data mapping and data discovery solutions are particularly

[90] Polonetsky, J. & Greenberg, J. (2019), NSF Convergence Accelerator: The Future of Privacy Technology, Future of Privacy Forum, Retrieved February 16, 2022 from https://fpf.org/wp-content/uploads/2020/03/NSF_FPF-REPORT_C-Accel1939288_Public.pdf.

[91] Privacy practices in the Indian technology ecosystem: A 2020 survey of the makers of products and services, (2020), Hasgeek, Retrieved February 16, 2022 from https://hasgeek.com/PrivacyMode/privacy-in-indian-tech-2020/.

[92] Jonnalagadda, K., Timothy, D. & Venkatanarayanan, A. (2021) Privacy practices in the Indian technology ecosystem, Hasgeek. Retrieved February 16, 2022 from https://hasgeek.com/PrivacyMode/privacy-in-indian-tech-2020/

[93] Arrka Infosec, Expert Techsource, Privacy Virtuoso Global and Sensorprol, (2021), See IAPP 2021 Tech Vendor Report, IAPP, Retrieved February 16, 2022 from https://iapp.org/media/pdf/resource_center/2021TechVendorReport.pdf

common. Secondly, companies dealing in specialised solutions may be less common, but certain companies like Doosra[94] and Truthshare,[95] are slowly gaining traction. Thirdly, various companies with a global presence are providing privacy- tech services in the country. A few of these are indigenous companies,[96] while some are based in other jurisdictions.[97] While various factors like ease of doing business and a hospitable regulatory regime in the country have encouraged these services, the development of privacy-tech in India still suffers from various supply-side challenges.

5.2.1 Lack of consensus on theoretical frameworks

In order for an industry to grow, a uniform theoretical framework on the solutions can be helpful.[98] Owing to the fact that it is still early days for the industry in India, the theoretical literature on the taxonomy of terms and the methodology to characterise privacy-tech is still underdeveloped. However, internationally, there is little consensus on taxonomy and methodologies for categorising privacy-tech.[99] The interpretation of certain terms differs according to laws, courts, privacy professionals, as well as vendors that self-preferentially develop terminology for marketing purposes. The lack of consensus is a major impediment to the growth of privacy-tech, which it can potentially slow down its development. Various issues including differences of understanding between the technology available in the market and the needs of buyers, the applicability of relevant laws, the development of technologies; as well as limited growth of platforms for knowledge sharing may come up.

Further, a lack of consensus on what technologies form part of the privacy-tech may cause uncertainty for stakeholders. For instance, consensus on the overlaps and distinctions between privacy technologies and cybersecurity solutions is still lacking. This has the potential to cause confusion for stakeholders producing insights including market reports as well as investors with limited portfolio capacities for privacy-tech solutions. One of the reasons for the lack of unanimity is the regular shifts in regulatory landscapes around the world. Data privacy frameworks are constantly evolving by either borrowing from other jurisdictions or departing from commonly accepted theoretical frameworks of taxonomy and methodologies for characterisation.[100] If left unaddressed, this may cause uncertainty among stakeholders and slow down the process of harmonising privacy-tech taxonomy.

[94] Doosra, Retrieved February 16, 2022 from https://www.doosra.com/.

[95] Truth Share, Retrieved February 16, 2022 from https://truthshare.com.ng/.

[96] Mindtree: A Larsen and Toubro Group Company, Retrieved February 16, 2022 from https://www.mindtree.com/services/data-and-intelligence/data-operations-and-management; TCS MasterCraft Dataplus, Retrieved February 16, 2022 from https://www.tcs.com/mastercraft/dataplus.

[97] Privacy and Data Protection (PDP) services: Key highlights of India's Personal Data Protection Bill (draft), 2018 (2018), Deloitte, Retrieved February 16, 2022 from https://www2.deloitte.com/in/en/pages/risk/articles/privacy-and-data-protection-services.html; Data privacy and AI protection, IBM, Retrieved February 16, 2022 from https://www.ibm.com/in-en/analytics/data-privacy-ai-protection.

[98] Privacy Tech's Third Generation: A Review of the Emerging Privacy Tech Sector, (June 2021), FPF, Retrieved February 16, 2022 from https://fpf.org/wp-content/uploads/2021/06/FPF-PTA-Report_Digital.pdf at 12.

[99] Privacy Tech Alliance et.al., (2021), Privacy Tech's Third Generation: A Review of the Emerging Privacy Tech Sector, Future of Privacy Forum, Retrieved February 16, 2022 from https://fpf.org/wp-content/uploads/2021/06/FPF-PTA-Report_Digital.pdf.

[100] Polonetsky, J. & Greenberg, J., (2019), NSF Convergence Accelerator: The Future of Privacy Technology, Future of Privacy Forum, Retrieved February 16, 2022 from https://fpf.org/wp-content/uploads/2020/03/NSF_FPF-REPORT_C-Accel1939288_Public.pdf at 27.

5.2.2 Shifts in regulatory landscape

Data privacy frameworks across various jurisdictions have witnessed regular shifts. In the United States, for instance, the data privacy landscape has changed significantly; with new laws coming up in California, Virginia and Colorado over the past few years. In January 2020, South Korea passed significant amendments to three of its data privacy laws, including its primary data privacy legislation, the Personal Information Protection Act.[101] In the same year, Singapore amended its Personal Data Protection Act, 2012 after several rounds of consultations; to enhance strictness.[102] In 2021, China enforced the Personal Information Protection Law, the country's first comprehensive data privacy law.[103] Earlier in 2022, China's new Data Security Law, which governs a wide range of data processing activities, also went into effect.[104]

Privacy- tech vendors have had to regularly adapt to ever-changing needs, causing multiple alterations and delays in creating feasible solutions. A regulatory regime that balances stability with adaptability can avoid uncertainty among vendors about expectations from their services. Further, it can enable consensus building among various stakeholders on the taxonomy and methodology to characterise privacy-tech.

5.2.3 Challenges pertaining to the growth of Artificial Intelligence

Artificial Intelligence plays an important role in the development of privacy-tech solutions in various jurisdictions. The need for the same arises since several privacy workflows currently are manual, making their implementation resource intensive. It is difficult to produce enough manpower to perform compliance tasks manually, and privacy professionals want technology to take over these duties so they can focus on more strategic initiatives.[105] For instance, data mapping and fulfilling data subject access requests are getting increasingly tough to operationalise manually, encouraging privacy professionals to look for appropriate privacy technology.[106] In addition to reducing workloads, the use of AI in privacy technology can help enable data ethics and compliance while ensuring data value creation. For instance, noise addition can fulfil differential privacy requirements or mask PII while still allowing machine learning to be run on data and create value.[107]

[101] Kang, C. & Kim, S. H., Recent major amendments to three South Korean data privacy laws and their implications, International Bar Association, Retrieved February 16, 2022 from https://www.ibanet.org/article/0D5FD702-179C-42A1-B37D-45D12F4556DA#:~:text=On%209%20January%202020%2C%20South,the%20Act%20on%20the%20Us.

[102] Angle, E., (2021, July 7) Singapore Makes Significant Changes to Data Privacy Legislation, Retrieved February 16, 2022 from https://www.epiqglobal.com/en-us/resource-center/articles/singapore-makes-changes-to-data-privacy,

[103] China's New Data Privacy Law is Sweeping and Serious: Avoid the High Cost of Noncompliance, The National Law Review (2021, August 24), Retrieved February 16, 2022 from https://www.natlawreview.com/article/china-s-new-data-privacy-law-sweeping-and-serious-avoid-high-cost-noncompliance.

[104] Kutner, A., et.al, (2021, December 2), China's New National Privacy Law: The PIPL, Mondaq, Retrieved February 16, 2022 from https://www.mondaq.com/china/data-protection/1137330/china39s-new-national-privacy-law-the-pipl

[105] IAPP 2021 Tech Vendor Report, (2021), IAPP, Retrieved February 16, 2022 from https://iapp.org/media/pdf/resource_center/2021TechVendorReport.pdf at 39.

[106] Ibid

[107] Privacy Tech's Third Generation: A Review of the Emerging Privacy Tech Sector, (2021), Future of Privacy Forum, Retrieved February 16, 2022 from https://fpf.org/wp-content/uploads/2021/06/FPF-PTA-Report_Digital.pdf at 23.

In the IAPP 2021 Tech Vendor Report, at least 38 vendors report using artificial intelligence in their solutions. The Indian market is also increasingly relying on AI to provide various solutions like data discovery,[108] digital risk management,[109] privacy management[110] and data classification.[111] It has been suggested that from as early as 2023, over 40% of privacy technology vendors will use AI,[112] which can help reduce administrative workloads while enabling value derivation out of data.[113] If this indeed is the case, impediments to the growth of AI in India need to be tackled. These challenges primarily pertain to talent, availability of data, monetisation and intellectual property.

According to the Global AI Talent Report, out of the 22,000 PhD-educated researchers in AI worldwide, only 386 are in India.[114] Further, serious research work in the field of AI is limited to less than 50 researchers with a concentration mostly in premier institutes like the Indian Institutes of Technology (IIT).

As identified in the National Strategy for AI as published by the NITI Aayog, the talent crunch leads to the low intensity of core research in fundamental AI technologies and the transformation of this research into market applications.[115] The government and the private sector have made efforts that provide a reason for optimism. For instance, the Government of Karnataka and NASSCOM have set up a Centre of Excellence for Data Science and AI.[116]

[108.] TCS MasterCraft Data Plus, (2021), See IAPP 2021 Tech Vendor Report, IAPP, Retrieved February 16, 2022 from https://iapp.org/media/pdf/resource_center/2021TechVendorReport.pdf at 215.

[108.] CloudSEK, See Shilpa Kumar et.al., (2021), Paving the Future: Why PrivacyTech is a rewarding frontier for venture capital, Omidyar Network India, Retrieved February 16, 2022 from https://www.omidyarnetwork.in/wp-content/uploads/Privacy-Tech-Thesis-July7.pdf. at 8.

[109.] Arrka Privacy Management Platform, ARRKA, Retrieved February 16, 2022 from https://arrka.com/Arrka-Privacy-Management-Platform; Overview, BORNEO, Retrieved February 16, 2022 from https://www.borneo.io/overview/.

[110.] Klassify, LinkedIn, Retrieved February 16, 2022 from https://www.linkedin.com/company/klassifytechnology/?originalSubdomain=in.

[111.] Gartner Says Over 40% of Privacy Compliance Technology Will Rely on Artificial Intelligence in the Next Three Years (2020, February 25), GARTNER, Retrieved February 16, 2022 from https://www.gartner.com/en/newsroom/press-releases/2020-02-25-gartner-says-over-40-percent-of-privacy-compliance-technology-will-rely-on-artificial-intelligence-in-the-next-three-years.

[112.] Gartner Says Over 40% of Privacy Compliance Technology Will Rely on Artificial Intelligence in the Next Three Years (2020, February 25), GARTNER, Retrieved February 16, 2022 from https://www.gartner.com/en/newsroom/press-releases/2020-02-25-gartner-says-over-40-percent-of-privacy-compliance-technology-will-rely-on-artificial-intelligence-in-the-next-three-years.

[113.] Privacy Tech Alliance and Future of Privacy Forum with Tim Sparapani and Justin Sherman, (2021), Privacy Tech's Third Generation: A Review of the Emerging Privacy Tech Sector, Future of Privacy Forum, Retrieved February 16, 2022 from https://fpf.org/wp-content/uploads/2021/06/FPF-PTA-Report_Digital.pdf at 9.

[114.] Dewan, N. (2019, June 18) In the race for AI supremacy, has India missed the bus?, The Economics Times, Retrieved February 16, 2022 from https://economictimes.indiatimes.com/small-biz/startups/features/in-the-race-for-ai-supremacy-has-india-missed-the-bus/articleshow/69836362.cms?from=mdr

[115.] National Strategy for Artificial Intelligence #AIFORALL, (2018) NITI Aayog, https://indiaai.gov.in/documents/pdf/NationalStrategy-for-AI-Discussion-Paper.pdf. at 46.

[116.] https://coe-dsai.nasscom.in

6 THE WAY FORWARD AND RECOMMENDATIONS

6.1 GOVERNMENT

The government (central and state) has a crucial role in incentivising privacy-tech businesses through enabling policies.[117] Governments support and incentivise technological innovation and start-up businesses through various central and state policies.[118] While it is ideal to extend those policies to privacy-tech businesses, key measures under various levers discussed in this chapter must be prioritised. Following sections discuss the levers under which the government can consider various measures and actions to aid privacy-tech businesses.

6.1.1 Regulatory Enablers

As discussed earlier, the enactment of the GDPR created compliance obligations that allowed the privacy technology market to develop. While providing services that guarantee the protection of individual privacy allows for greater traction among consumers, the role that regulation plays simply by introducing compliance standards must not be underestimated. With the evolution of India's data protection landscape, and the introduction of the Digital Personal Data Protection Bill, 2022 it is likely that we are going to see a rapid increase in privacy-tech vendors within the market.

The government can also enable ease of doing privacy-tech business through enhancing and relaxing regulatory requirements, compliance, and due diligence. As step one, governments should consider establishing a separate nodal agency for privacy-tech or a division under Start-up India Initiative[119] that would act as a single-window for clearance for exemptions, incentives and grievance redressal. Similarly, the government can provide knowledge support to privacy-tech businesses by providing access to the National Science, Technology, Innovation Observatory,[120] as envisioned under the draft Science, Technology, Innovation Policy 2020.[121]

6.1.1.1 Limited Regulatory Exemptions

On the compliance front, governments can aid privacy-tech businesses by exempting them from specific regulations or accepting self-certification under those regulations. For instance, the labour regulation of Kerala is simplified for Information Technology/Information

[117] Government intervention for enabling the market and supporting privacy is a facet of market development. However, various factors such as geographical constraints, cultural barriers, political instability, lack of demand for innovation and supply of raw material, etc., determine India's performance in enabling technological innovation like privacy tech.

[118] https://www.startupindia.gov.in/

[119] Ibid

[120] Central repository for all kinds of data related to and generated from the STI ecosystem, including information on all financial schemes, programmes, grants and incentives that exist in the ecosystem.

[121] Science, Technology, and Innovation Policy. (2020, December 4). Department Of Science & Technology. Retrieved January 20, 2022, from https://www.psa.gov.in/psa-prod/psa_custom_files/STIP_Doc_1.4_Dec2020.pdf

Technology-enabled (IT/ITeS) businesses.[122] Besides, the governments must allow privacy-tech businesses to get recognised by the Department for Promotion of Industry and Internal Trade as start-ups to get various benefits.[123] Additionally, the government can aid privacy-tech businesses, by incorporating privacy as an element in pre-investment due diligence[127] mandated by the Securities Exchange Board of India under the Securities Exchange Board of India (Alternative Investment Funds) (Second Amendment) Regulations, 2021.[128]

6.1.1.2 Intellectual Property

Secondly, governments can also consider creating a secure environment for privacy-tech businesses by enhancing laws related to intellectual property rights (IPR). To enjoy IPR protections in India, businesses must register under the Patents Act, 1970, Trademarks Act, 1999 and the Copyright Act, 1957.[124] While the patent law was amended in 2005 and various Rules under these legislations have been proposed in recent days, still most of the core IPR related legislations are old, predating most technology developments. India is currently ranked 57th in the Global Competitiveness Index that evaluates intellectual property protection across 141 jurisdictions globally,[125] which is lower than some of its South Asian peers like Indonesia. On the implementation front, the absence of trade secrets law,[126] as part of IPR legislation is suboptimal as it necessitates businesses to take recourse through a slow process of judicial proceedings to protect confidential business information.

6.1.1.3 Sandboxes

Thirdly, the government can set up a sandbox mechanism to accommodate privacy-tech. By establishing a sandbox mechanism, the government can allow privacy-tech businesses to test their innovations against the set principles notified by the regulator without the risk of violations. The sandbox mechanism is already used by central, state governments and regulatory bodies in India. For instance, the Reserve Bank of India (RBI) introduced the Regulatory Sandbox in 2019. This sandbox aims to bring innovation in financial services by allowing businesses to live-test their solutions in a controlled regulatory environment.[129] Since 2019, RBI has hosted four regulatory sandbox cohorts on retail payments[130] (six

[122] Kerala Technology innovation and entrepreneurship policy .(2017) Retrieved from https://www.startupindia.gov.in/content/dam/invest-india/Templates/public/Kerala%20Startup%20Pollcy%202017.pdf

[123] Startup India Kit. (2021, June 30). Startup India. Retrieved January 20, 2022, from https://www.startupindia.gov.in/content/dam/invest-india/Templates/public/Updated%20SUI%20Kit_170921.pdf

[124] Intellectual property rights in India. (n.d.). GOV.UK. Retrieved January 20, 2022, from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/627956/IP-Rights-in-India.pdf

[125] The Global Competitiveness Report 2019. (n.d.). weforum.org. Retrieved January 20, 2022, from https://www3.weforum.org/docs/WEF_TheGlobalCompetitivenessReport2019.pdf

[126] Sanadhya, N. (2020, June 9). Protecting Trade Secrets In India In The Absence Of A Regime. Khurana & Khurana Advocates and IP Attorneys. Retrieved January 7, 2022, from https://www.khuranaandkhurana.com/2020/06/09/protecting-trade-secrets-in-india-in-the-absence-of-a-regime/

[127] Unlocking The Potential of India's Data Economy: Practises, Privacy And Governance. (2021). Deloitte. https://www2.deloitte.com/content/dam/Deloitte/in/Documents/about-deloitte/Privacy_and_Data_Ethics-A_Roadmap_for_India_Report_V4.pdf

[128] Securities and Exchange Board of India (Alternative Investment Funds) (Second Amendment) Regulations, 2021

[129] Enabling Framework for Regulatory Sandbox. (2019, August 13). Reserve Bank of India. Retrieved January 21, 2022, from https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=938

[130] Regulatory Sandbox (RS): First Cohort on 'Retail Payments' – Exit. (2021, September 13). Reserve Bank of India. Retrieved January 21, 2022, from https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=52217

entities successfully exited), cross border payments,[131] MSME lending[132] and prevention and mitigation of financial fraud.[133] Similarly, Singapore launched a PET Sandbox in July 2022 to allow PET service providers to develop relevant use cases, which may include the use of PETs to increase efficiency in healthcare and a more general whole-of-government approach and to pilot PETs.

6.1.1.4 Taxonomy

Finally, the governments can aid privacy-tech businesses with two key concerns, i.e., lack of clarity and consensus (a) in the definition of privacy-tech and other related terms[134] (b) readiness and quality of privacy-tech.[135] The central government can clearly define key terminologies like privacy-tech, privacy-enabling technologies, and privacy-preserving technology along with defining the regulatory thresholds for compliance. In addition, the governments at both the central and the state levels can resort to the market mechanisms such as accreditation and certification[136] for privacy-tech businesses. A notable example is that of Singapore, where a Digital Trust Centre has been launched at Nanyang Technological University to study PETs further.[160]

6.1.3 Incentives

The government can bestow privacy-tech businesses with various incentives infrastructurally and in kind (indirect monetary benefits) as an agency to enable innovation. Starting from infrastructural support, state governments must consider privacy-tech businesses as start-ups within the IT/ITeS sector, such that they get access to existing infrastructures like, start-up parks, IT parks, innovation hubs, etc. For instance, the Haryana government has provided suitable infrastructural support through an innovation hub in Gurugram over 30,000 sq. ft land[137] with a start-up warehouse, Mobile Application Centre, United Nation Technology & Innovation lab and Internet of Things (IoT) Centre.

Besides, governments must also consider setting up incubator facilities that provide office space, training, networking opportunities and financing. Various state governments have established incubator hubs in the country. For instance, in 2017, the Kerala government established Kerala Technology Innovation Zone[138] - an integrated incubator hub for multiple domains and technology sectors under a single roof, which currently houses 500 start-ups. In addition to this, the Kerala government established a federated Fab network

[131] Regulatory Sandbox (RS): Second Cohort on Cross Border Payments – Test Phase. (2021, September 13). Reserve Bank of India. Retrieved January 21, 2022, from https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=52218

[132] Reserve Bank Announces Opening of Third Cohort under the Regulatory Sandbox. (2021, September 13). Reserve Bank of India. Retrieved January 21, 2022, from https://www.rbi.org.in/scripts/FS_PressRelease.aspx?prid=52219&fn=9

[133] RBIs fourth regulatory sandbox cohort is on prevention of financial frauds. (2021, October 9). Business Standard. Retrieved January 21, 2022, from https://www.business-standard.com/article/finance/rbi-s-fourth-regulatory-sandbox-cohort-is-on-prevention-of-financial-frauds-121100900048_1.html

[134] Privacy Tech's Third Generation A Review of the Emerging Privacy Tech Sector. (2021). Future of Privacy Forum. https://fpf.org/wp-content/uploads/2021/06/FPF-PTA-Report_Digital.pdf

[135] Ibid

[136] Hansen, M., Hoepman, J.-H., & Jensen, M. (2016). Towards Measuring Maturity of Privacy-Enhancing Technologies. Annual Privacy Forum, 9484, pp 3-20. https://link.springer.com/chapter/10.1007/978-3-319-31456-3_1

[137] Entrepreneur and Startup Policy 2017. (n.d.). Startup Haryana. Retrieved January 7, 2022, from https://startupharyana.gov.in/files/startup-policy_final_28th-sep.pdf

[138] Kerala Technology Innovation Zone. (n.d.). Retrieved from https://innovationzone.in/

that branches into 21 mini-fab labs across Tier II and Tier III locations to encourage innovation, technology development, product prototyping, market learning, and commercial product development.[139] Access to these existing incubator hubs and centres established by governments must be extended to privacy-tech businesses.

6.1.4 Fiscal support

The government can consider providing financial support across the life cycle of the privacy-tech business through both direct and indirect funding. Considering privacy-tech businesses follow the life cycle of start-ups, they go through five stages in business development – ideation (pre-seeding), concept (seeding), commercialisation, expansion, and exit. Privacy-tech needs government support during the challenging phase of the ideation, concept, and commercialisation stage.

At the ideation stage, privacy-tech businesses do the groundwork, legal analysis, and market research to develop viable technological solutions. During this stage, the government can consider stimulating innovation by organising competitions on privacy and data protection issues and providing fiscal incentives for best solutions. For instance, the Tamil Nadu government has instituted the Open Innovation portal,[140] for posting governance, societal and industrial challenges needing innovative solutions in the public domain. Under this initiative, recently, the government awarded multi-channel vaccine portal technology as the best innovation, developed by GoFloaters in response to the problem faced by Coimbatore Municipal Corporation in vaccine distribution.[141] While challenges and competition provide indirect support, the government can also directly fund innovative ideas of privacy-tech businesses through seed funding.[142]

Next in the pipeline is the concept stage. This is the most crucial phase of the privacy-tech businesses as they develop the solution prototype. Funding support at this stage is essential for privacy-tech businesses to move towards commercialisation. The government can fund prototype development followed by funding the soft launch of the viable solution and scale up the same. In addition to funding, the government can also use other financial instruments for supporting privacy-tech like, collateral-free loans, insurance, equity funds, credit guarantee, etc. An instance of this lies in the Rajasthan government's Bhamashah Techno Fund[143] of Rs. 500 crores for providing collateral-free loans[144] and equity funds to start-ups at any stage. The central government and SIDBI's Credit Guarantee Fund Trust for Micro and Small Enterprises provide partial collateral security through guarantee cover for credit facilities uncovered by collateral security.[145] Availability of appropriate and suitable financial products and services at the concept stage will bring financial stability[146] to the privacy-tech businesses, such that they concentrate on scaling

[139] Kerala Technology Startup Policy. (2014). Retrieved from https://jecc.ac.in/documents/Kerala_Technology_Startup_Policy.pdf

[140] Tamil Nadu Startup & Innovation Policy. (n.d.). editn.in. Retrieved January 7, 2022, from https://www.editn.in/app/webroot/img/ATI/STARTUP-TN%20Policy.pdf

[141] GoFloaters wins innovation challenge. (2021, December 5). The Hindu. Retrieved January 22, 2022, from https://www.thehindu.com/news/cities/Coimbatore/gofloaters-wins-innovation-challenge/article37846600.ece

[142] Seed funding support can be extended until commercialisation stage.

[143] Bhamashah Techno Fund. (n.d.). Retrieved from https://istart.rajasthan.gov.in/pages/bhamashahtechnofund

[144] Based on Qrate ranking

[145] Credit Guarantee Fund Scheme for MICRO AND SMALL ENTERPRISES. (n.d.). MSME. Retrieved January 7, 2022, from https://msme.gov.in/sites/default/files/CredirGuranteeFundScheme_1.pdf

up to move towards commercialisation.

Moving to the commercialisation stage of the technological solution, until the privacy-tech businesses capture their market share, the government can support the privacy-tech businesses by enabling investment in the form of (a) alternative investment funds where the government can hold a partnership, or (b) standard investment subsidies on fixed capital investment.[147] Besides, the government can consider providing various fiscal incentives to privacy-tech businesses at the commercialisation stage. Directly through reimbursements, tax holidays, power cost exemptions, operational subsidies, grants, allowances, etc. For instance, the Maharashtra government covers 80% of the quality testing cost at Bureau for Indian Standards (BIS) accredited facilities.[148]

6.1.5 Competence building

To ramp up the knowledge quotient of privacy-tech businesses, governments can provide mentoring support and knowledge-sharing mechanisms. A holistic mentoring facility where the privacy-tech businesses get end-to-end mentoring can aid them in understanding the nuances of data protection, and privacy void they can fill with their solutions, etc. A similar measure has been tried in Kerala, where the government has established Future Research labs to upskill entrepreneurs with core technologies like machine learning, big data, etc. Moving away from subject-specific knowledge, the government can institute information centres for privacy-tech businesses to understand the formalities of filing intellectual property rights and patents. Rajasthan government envisions similar measures through its drafted Start-up and Innovation Policy, 2019,[149] connecting start-ups to patent information centres to understand the formalities of filing intellectual property rights. Australia provides training resources that can be used within programmes built by private entities and highlight a helpful point of entry through its video resources.[150]

6.2 PRIVATE ENTERPRISES

6.2.1 A shift in cultural factors

A privacy-centric culture that prioritises the protection of user privacy has the potential to fulfil various objectives of the company. Organisations need to start thinking of legislative compliance, cyber security and privacy protection as complementary goals. In order to achieve this, the following recommendations can be considered. Firstly, the increased buy-in of the leadership in privacy governance can be helpful. Existing efforts by executives like incorporating data security and privacy as a part of corporate governance strategies

[146] Ananth, B., & Mor, N. (2009, June 24). Finance as Noise-Cancelling Headphones - WSJ. Wall Street Journal. Retrieved January 22, 2022, from https://www.wsj.com/articles/SB124581691732345881

[147] Acquisition and maintenance of long-term tangible and intangible assets

[148] Maharashtra State Innovative Startup Policy. (2018). Retrieved from https://www.startupindia.gov.in/content/dam/invest-india/Templates/public/state_startup_policies/Maharashtra_State_Innovative_Startup_Policy_2018.pdf

[149] Rajasthan Start-up Ecosystem Report. (2019). Retrieved from https://www.rajras.in/rajasthan-startup-ecosystem-report-2019/

[150] Training Resources, O°ce of the A ustralian Information Commissioner, from https://www.oaic.gov.au/privacy/training-resources

and creating sub-committees for looking into privacy concerns need to be strengthened through regular assessments and focus on accountability. Further, a team focused on the protection of user privacy can be introduced within the company.

The disproportionate focus on minimising corporate risk often encourages many companies to house their privacy officers within other risk management departments.[151] The EY IAPP 2021 Annual Privacy Governance Report revealed that the privacy team is most likely to be housed within the legal department, followed by its security and IT teams. Only in 10% of cases was a specific privacy and data protection team responsible for privacy mandates.[152] There should be an impetus to shift the focus to the protection of consumer privacy by, for instance, creating a privacy department separate from the legal, IT and risk teams. This team can directly report to the top decision-makers and ensure that user privacy directly affects design decisions before they are finalised as a technological fix.

Secondly, awareness of privacy-tech solutions needs to be facilitated. In order to make informed decisions about adopting privacy- tech, companies need to work on capacity building of internal stakeholders. An effective privacy training program driven by privacy-by-design principles like full lifecycle protection and transparency[153] can successfully communicate the significance of protecting user privacy and privacy compliance. It is important that the training is not a mere box-ticking exercise but trains employees to respond to real-life situations. For instance, the course of action in case of a data leak and the manner of responding to privacy complaints from users should be taught through live demonstrations and product variants. Employees should be taught the manner in which certain privacy-tech solutions can be meaningfully utilised in these situations. This will help employees realise the practical value of privacy-tech solutions, rather than merely providing a theoretical understanding.

Thirdly, considering the prevalence of legal endogeneity in privacy-tech, companies should do their due diligence[154] to ensure that the solutions they incorporate do not disproportionately focus on avoiding managerial risk and instead keep the privacy interests of users in mind. It would also be prudent to make use of privacy information providers like TeachPrivacy and DataGuidance that work with lawyers to provide information necessary for legal compliance.[155]

Fourthly, priority should be given to the identification of those privacy-tech solutions that specifically correspond to the needs of the business. It is not necessary to be aware of every state-of-the-art privacy tech solution in the market. For instance, if companies are looking to enhance their privacy capacities at certain stages of the data lifecycle, the focus should be on identifying appropriate PETs. For a company in its initial stages of privacy tech investment, it may be prudent to focus on foundational privacy-tech services. Fundamental processes in the data processing lifecycle should be protected through solutions like data

[151] Waldman, Ari Ezra, Privacy Law's False Promise (2019, December 6), Washington University Law Review, Vol. 97, No. 2, 2020, Retrieved February 16, 2022 from SSRN: https://ssrn.com/abstract=3499913

[152] IAPP-EY Annual Privacy Governance Report 2021 (2021), IAPP, Retrieved February 16, 2022, from https://iapp.org/media/pdf/resource_center/IAPP_EY_Annual_Privacy_Governance_Report_2021.pdf

[153] Privacy by Design. (n.d.). Information and Privacy Commissioner of Ontario. Retrieved October 20, 2022, from https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf

[154] Waldman, A., Privacy Law's False Promise (2019, December 6). Washington University Law Review, Vol. 97, No. 2, 2020, Retrieved February 16, 2022 from SSRN: https://ssrn.com/abstract=3499913

[155] Ibid

mapping before looking at complicated solutions like homomorphic encryption.

Lastly, privacy-safe value derivation from data should be encouraged. For instance, solutions that can map the movement of data within the organisation can ensure that data does not go unnoticed and can inform the analysis. Simultaneously, it can help avoid unauthorised access to data by various internal or external stakeholders. Further, data auditing technologies can enable data minimisation by deleting unnecessary data and derive value by ensuring that out-of-date data does not inform the company's analysis.

6.2.2 Internal processes

To seamlessly integrate privacy-tech solutions, relevant internal processes may need to be established or amended. For instance, mechanisms to resolve disputes on decisions pertaining to user privacy need to be established. Dispute System Design (DSD) has gained traction over time to create organisational strategies for conflict management. The strategy includes four integral steps, i.e., diagnosis of dispute symptoms, design of a strategy that minimises cost and prioritises less invasive approaches, the implementation by ensuring that relevant stakeholders are on board, and a careful evaluation of the design strategy adopted.[156]

Further, pilot testing procedures; including feasibility assessments for privacy- tech solutions can be incorporated to ensure smooth integration. These procedures need to not only look at the short-term implications of the technology but also, the long-term impact on the organisation's success and sustainability.[157] It is also crucial that any assessment analyses the impact on the organisation's culture and its effect on outcomes for privacy including accountability mechanisms. Further, the incorporation of mechanisms like access control, wherein internal stakeholders are provided access to data on the basis of their roles or functions, can introduce users to the relevance of internal processes in ensuring data privacy. Establishing access control policies can provide consistency, clarity and sustainability with the objective of preventing unauthorised access to data.

6.2.3 Budgetary restrictions

Budgetary allocations for privacy- tech can increase if companies realise the financial benefits of the solutions and a comprehensive view of requirements is taken. While considering the Return on Investment of privacy-tech, companies should attempt to look beyond the money saved on fines for non-compliance. Financial benefits that can accrue by preventing data breaches, making operations more efficient, reducing sales delays and deriving value out of data should also be considered to make a strong case for adopting privacy- tech. Data retention solutions like 'Encryption in Rest', for example, can help ensure that sensitive user data does not fall prey to leaks. Analysing data on privacy spending and benefits, Cisco's report estimates that for every dollar of investment, a company makes, it receives $2.70 worth of benefits. The study revealed that 47% of

[156]. Staˆ , P. (2022, Jan. 3), What is a Dispute System Design?, Harvard Law School,, Retrieved February 16, 2022 from https://www.pon.harvard.edu/daily/dispute-resolution/what-is-dispute-system-design/.

[157]. Berry, G. & Shabana, K., Adding a strategic lens to feasibility analysis (2021), New England Journal of Entrepreneurship, Vol. 24, No. 1, 2021, Retrieved February 16, 2022 from https://www.emerald.com/insight/content/doi/10.1108/NEJE-08-2019-0036/full/pdf?title=adding-a-strategic-lens-to-feasibility-analysis.

companies see more than the twofold return on privacy investments, 33% are breaking even, and only 8% spent more than they are receiving back in benefits.[158]

Budget decisions need to be taken after taking a holistic view of company financials and requirements. For instance, companies with limited budgets and basic needs can look at solutions with multiple offerings. Comprehensive solutions in the market with various offerings like data subject access requests and data mapping can be considered.[159] As discussed earlier, companies like IBM offer suits of services which include important technologies like data labelling and annotation. On the other hand, companies with unique requirements can consider spending more on hyper-specific solutions. Companies which extensively undertake data sharing with third parties can consider digital watermarking solutions to monitor the data transferred and prevent unauthorised sharing. Further, the distribution of privacy budgets needs to be reviewed periodically, in line with company requirements and future objectives. Currently, a majority of the privacy budget is spent on salaries, benefits, and outside counsel while a meagre 11% is being spent on technology and tools.[160] Technology that can save labour and affordably protect user privacy should be given an increased focus on privacy budgets.

6.3 INVESTORS

Investors have a dual role to play in fostering the growth of privacy-tech in the country. First, they can play a more active part in ensuring privacy-centric practices in their portfolio companies. Secondly, they can facilitate the development of privacy-tech in the country by investing in solutions fit for the Indian market. Both these aspects have been important trends in the venture capital space.[161]

6.3.1 Privacy protection as a value addition

Privacy compliance is becoming an increasingly important concern for investors while making investment decisions[162] and guiding their portfolio companies. However, the current approach is to look at data privacy as a hygiene criterion rather than a strategic one, with a focus on regulatory compliance.[163] Investors should ascertain that potential portfolio companies can derive optimum value out of data in a sustainable and privacy-centric

[158] White Paper on Privacy Gains: Business Benefits of Privacy Investment (2019), Cisco, Retrieved February 16, 2022 from https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/privacy-gains-business-benefits-of-privacy-investm ent-white-paper.pdf.

[159] 2021 Tech Vendor Report, (2021, September), IAPP, Retrieved February 16, 2022 from https://iapp.org/media/pdf/resource_center/2021TechVendorReport.pdf

[160] IAPP-EY Annual Privacy Governance Report 2021 (2021), IAPP, Retrieved February 16, 2022 from https://iapp.org/media/pdf/resource_center/IAPP_EY_Annual_Privacy_Governance_Report_2021.pdf,

[161] Pfeifle, S. (2015, May 11), VCs: Data Privacy Aˆects Y our Valuation, Ability To Raise Capital, IAPP, Retrieved February 16, 2022 from https://iapp.org/news/a/vcs-data-privacy-aˆects-your-valuation-ability-to-raise-capital/); See also Kuranda, S. (2018, September 12), Venture capitalists increasingly investing in privacy tech, IAPP, Retrieved February 16, 2022 from https://iapp.org/news/a/venture-capitalists-increasingly-investing-in-privacy-tech/.

[162] Pfiefle, S. (2015, May 11), VCs: Privacy aˆects your valuation, ability to raise capital, IAPP R etrieved February 16, 2022 from https://iapp.org/news/a/vcs-data-privacy-aˆects-your-valuation-ability-to-raise-capital/.

[163] Unlocking the potential of India's data economy: practices, privacy and governance (2019), Deloitte, Retrieved February 16, 2022 from https://www2.deloitte.com/content/dam/Deloitte/in/Documents/about-deloitte/Privacy_and_Data_Ethics-A_Roadmap_for_India_Report_V4.pdf

manner. These can be done by providing technical guidance on privacy practices and technology, routine privacy audits[164] or periodic assessments.

Investors can also focus on standardising expectations[165] and taxonomy between them and businesses when it comes to referencing privacy practices and solutions. From mechanisms of privacy audits and metrics to decision-making at the board level, it is necessary that both stakeholders are on the same page. Classifications on the basis of the data processing lifecycle or the technology's ability to preserve or enhance privacy may be used as foundations to build consistent terminologies. These can also help gradually develop consensus on the theoretical framework of privacy-tech. In order to achieve this, advice and counsel from privacy professionals and tech vendors may be taken.

While early-stage start-ups are still focused on refining the core business model and scalability, investors must also help these start-ups to incorporate privacy solutions from the very start.[166] Early adoption can ensure a smooth incorporation experience and avoid the compulsion of making significant operational changes at a later stage. This would also drive home the idea that privacy is not a matter of just regulatory compliance, but a vital cog of the business model itself. Investment decisions must not just consider the capacity to comply with regulatory obligations in the future, but also in the present. Such investment decisions may vary sectorally, and as per the maturity of the start-ups in consideration, so, departing from a one-size-fits-all philosophy may be prudent.

6.3.2 Growth of context-appropriate privacy-tech start-ups

On the supply side, investors need to prioritise funding of those privacy-tech solutions which are appropriate for the maturity of the Indian market and adaptable to the current Indian regulatory framework. Easy-to-integrate solutions that take care of foundational processes of the data lifecycle can be encouraged. Further, the focus should be given to low-cost technologies that can be conveniently afforded by most businesses. Attention should be on building privacy protection capacities of the tech industry as a whole, rather than a few big players. It is also crucial that privacy-tech vendors are able and willing to adapt to constantly evolving regulatory frameworks globally.[167] Therefore, investors should look for start-ups that can amend their solutions as and when needed.

[164] Unlocking the potential of India's data economy: practices, privacy and governance (2019), Deloitte, Retrieved February 16, 2022 from https://www2.deloitte.com/content/dam/Deloitte/in/Documents/about-deloitte/Privacy_and_Data_Ethics-A_Roadmap_for_India_Report_V4.pdf

[165] Pipikaite, A. (2018, December 19), Here Are Four Diˆerent W ays Investors Can Influence More Secure and Responsible Innovation, The World Economic Forum, Retrieved February 16, 2022 from https://www.weforum.org/agenda/2018/12/four-ways-investors-influence-more-secure-responsible-innovation/.

[166] Palme, S., (2021, April 13), Data Protection & Venture Capital: Does Privacy compliance influence investment decisions into start-ups?, Palqee, Retrieved February 16, 2022 from https://www.palqee.com/blog/2021/data-protection-and-venture-capital/.

[167] Epiqu (2021, August 11), U.S. Data Privacy Roundup- What is on the Horizon, Jdsupra, Retrieved February 16, 2022 from https://www.jdsupra.com/legalnews/u-s-data-privacy-roundup-what-is-on-the-6247901/; Boardman R., & Nevola C. (2021, October 15), Changing direction? UK Consults reforms to its data protection law, IAPP, Retrieved February 16, 2022 from https://iapp.org/news/a/changing-direction-uk-consults-reforms-to-its-data-protection-law/.

6.4 CIVIL SOCIETY

The privacy paradox describes an inconsistency between the apprehensions of people regarding their privacy and their actual behaviour. While users are concerned about their privacy, they do not actually do a lot to protect their privacy. The privacy paradox has held back user demand for adequate protection of privacy from companies. The paradox has been attributed to various reasons including knowledge deficiency[168] about privacy-protecting practices. Civil society has an important role to play in ensuring that the sentiment shifts from a general expectation of data privacy to making privacy protection an important determinant while buying technological solutions[169] through knowledge enhancement. Literature and tools aimed at explaining concepts pertaining to privacy, e.g., encryption and informed consent ii highlighting the nature of the information collected by companies iii curating easily deployable strategies to give consumers more control over their data sharing and iv creating parameters to measure the privacy-protecting capacities of data fiduciaries should be developed and disseminated.

Currently, various organisations are providing useful interventions in this direction. The Electronic Frontier Foundation has curated a series of tools that spots and blocks third-party domains that track browsing habits.[170] IAPP has routinely published research aimed at educating users about the manner in which their data is shared by various stakeholders[171] and the state of data privacy of Indian mobile apps and websites.[172] Mozilla Foundation’s buyers guide rates products on the basis of how privately and securely they keep user data.[173] Civil society has a role to play in the growth and increased adoption of privacy-tech beyond the resolution of the privacy paradox as well. There is a need to analyse the efficiency of solutions that can enhance privacy outcomes and encourage their adoption by companies.

7 A FRAMEWORK TO UNDERSTAND PRIVACY-TECHNOLOGY READINESS OF FIRMS

In the specific Indian context, while privacy concern remains to be one of the key concerns considered by the markets, however less clarity in terms of how this translates into proactive engineering. This is because of the lack of (a) industry coherence

[168] Bilal A. et. al. (2020), Virtue Ethics as a Solution to the Privacy Paradox and Trust in Emerging Technologies, Retrieved February 16, 2022 from https://www.researchgate.net/publication/341041506_Virtue_Ethics_as_a_Solution_to_the_Privacy_Paradox_and_Trust_in_Emerging_Technologies.

[169] Tsai J. et al (2020), Effect of Online Privacy Information on purchasing behaviour: an experimental study , Heinz, Retrieved February 16, 2022 from https://www.heinz.cmu.edu/~acquisti/papers/acquisti-onlinepurchasing-privacy.pdf

[170] Gebhart G. (2016, September 27), Five EFF tools to help you protect yourself online, EFF, Retrieved February 16, 2022 from https://www.eff.org/deeplinks/2016/09/five-eff-tools-help-you-protect-yourself-online

[171] Shenkman C. et al. (2021, December), Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers, IAPP, Retrieved February 16, 2022 from https://iapp.org/resources/article/legal-loopholes-and-data-for-dollars-how-law-enforcement-and-intelligence-agencies-are-buying-your-data-from-brokers/

[172] State of data privacy of Indian mobile apps and websites (2020), Arrka , Retrieved February 16, 2022 from https://iapp.org/media/pdf/resource_center/state_privacy_apps_websites_india_2020.pdf

[173] Privacy not included, Mozilla Foundation, Retrieved February 16, 2022 from https://foundation.mozilla.org/en/privacynotincluded

in the approach, (b) standard vernacular which can translate Indian law into technical "must-haves", (c) understanding of adequate budgets for effective privacy-engineering and (d) the practical knowledge of first steps needed to prepare. The readiness framework discussed in this chapter attempts to provide the zero-to-one flow needed for the successful management of a typical data-intensive company in an environment where data protection is both a legal obligation as well as a user expectation. The framework will help majorly with the obstacles outlined in (d), (a), and to a lesser extent with (b) and (c).

7.1 THE DATA BALANCE SHEET

The need for a proactive and planned trajectory for privacy engineering comes from the recognition that data is both an asset and liability, and not just a resource or raw material that can be extracted, processed, and can be discarded without any consequences to organisations and individuals. Hence, a balance sheet approach to thinking about data is needed, where the data collected appears simultaneously in the asset and liability ledgers.

The asset side of the data ledger can be visualised as follows:

While the first three steps are expenses incurred to create the asset (data), the final step allows the creation of monetisable products. It allows for granular control of the asset production process either through ancillary data (also referred to as processed data) or through insights obtained either by analytics or by creating and training machine learning models on the primary data for service delivery. Dual production of data value is considered the dominant business model, particularly for firms that are organised as platforms and other firms that are trying to derive revenue from data. This means that both primary and ancillary data can be useful in two different ways – one having a value in how the primary service may be improved due to better insights about the service, and two, having value as a data point that is important to other organisations to target their products or improve their market intelligence.

The liability side of data is difficult to abstract because the utility of data is impacted by the passage of time (currency effect). Current data practices are largely speculative in collection and monetisation. A necessary time lag in valuation is a significant feature of current data valuation practices. This has adverse implications on any process that benefits from an a priori need to estimate the value of collected data. This can include growth estimates, risk assessments for compliance and impact assessments for sustainability and, in the present case, privacy engineering. For instance, consider the example of the credit score of an individual. Credit agencies not only adjust the score based on financial transactions under-taken but also because of regulatory guidance.[174]

[174]. Bhasin, T. (2020, May 22). Your credit score may change under new Cibil scoring method. Mint. Retrieved February 16, 2022, from https://www.livemint.com/money/personal-finance/your-credit-score-may-drop-as-cibil-changes-scoring-method-11590137077603.html

BOX 2

Time Value of Data

The concept of 'time value of data' usually denotes that the value of data reduces over time.[175] For instance, the data about a user's shopping history will be relevant for advertisers a few minutes or hours after the online activity. However, the relevance or utility of the data reduces for the advertiser as time passes because, among other things, the preference of the user is likely to change over time. Simply put, there is a timeliness or 'currency' component to the value of data, i.e., the value of information is related to time, and that value may degrade as time elapses.[176]

- To get the greater value of data, business analytics need to be informed by data as quickly as possible.[177]
- The growing threat of ransomware has established insurance players to move away from cyber insurance, as the liabilities are difficult to measure.
- Lack of insurance coverage would have financial implications in case of a breach, such as cash flow crunch and asset-liability mismatches.
- Attacks on the firms operating downstream in the supply chain commonly use open-source software, which is cumbersome to monitor and hence makes a breach highly likely in the medium-long term.
- Regulations that govern data management, processing, consumer protection, and breach notifications, which are highly country-specific and sector-specific and hence have significant variability in estimating liability.
- Institutional structures that enforce these regulations and their credibility and capability. If they are weak, then liabilities are under-estimated, but if they are too strong, liabilities are overestimated.

The variability in valuation presents a problem, particularly because businesses in the dominant shareholder paradigm of control are incentivised by their shareholders to increase both their assets and revenue generation from the assets in the short-term, and simultaneously reduce their liability and related expenses. When liability is hard to estimate, it is typically underestimated, as it is perceived as an abstract construct that has not yet materialised in Indian conditions.

Hence, expenses that are incurred (or estimated) to reduce the liability are given a smaller share in the budget planning exercise and are treated very differently compared to expenses incurred for revenue generation. This means privacy engineering and any technological solution that is being rolled out, in the current scenario, must always satisfy the following criteria:

[175] Henson, T., Garcia, F., Sainsbury, C., & Burt, P. (2018, March 30). Explaining the Time Value of Data. Dell. Retrieved February 16, 2022, from https://www.dell.com/en-us/blog/explaining-time-value-of-data/

[176] Moody, D., & Walsh, P. (2003, May 26). The Value of Business Intelligence. CDN. Retrieved February 16, 2022, from https://cdn.ttgtmedia.com/searchSMB/downloads/LoshinBusIntelchap2.pdf

[177] Bean, R. (2018, July 24). Time to Value: The Currency of Data Operations. Forbes. Retrieved February 16, 2022, from https://www.forbes.com/sites/ciocentral/2018/07/24/time-to-value-the-currency-of-data-operations/

1. Suitably priced at the point of purchase as it must fit within a limited budget.
2. It cannot create friction in the business-as-usual development processes.
3. Value generation in terms of identifying issues, or in simpler terms, the demonstration of value must be near-instantaneous for subsequent budget allocation on a recurring basis.
4. Local and sectoral legislation cannot be hardcoded because of jurisdictional differences, and the non-local nature of data must be flexible enough to accommodate them. The technology must possess the capacity for legal retrofitting – i.e., broadly compliant in a basic form that is in line with the general global privacy legislation.
5. Violations, if flagged, cannot be abstract, but must be mapped into existing laws and regulations at a dashboard level, as mere technical indications are not enough and would be ignored.

BOX 3

Dashboard View

A dashboard view refers to a user interface that provides a visual interface of key indicators.[178] The interface is typically utilised to present an easily understandable and at-a-glance view of relevant indicators. In the context of data privacy, dashboards have been adopted in two major ways. Firstly, they have been implemented as an interface by various tech companies to provide data subjects information about their privacy settings, enabling data privacy compliance.[179] Secondly, dashboards have been incorporated by privacy-tech vendors in their enterprise solutions. These dashboards allow companies to understand key indicators pertaining to data privacy, including compliance. For instance, CipherCloud's dashboard provides information on data usage, volume and risk level,[180] and ConsentEye's board provides a real-time risk register for the data protection officer.[181] Certain solutions like 4Comply map the dashboard extensively with privacy laws, providing a map of countries and respective compliance statuses.[182] The primary purpose of a dashboard view is, therefore, to provide a readily consumable overview of privacy compliance that can inform privacy governance within a company.

[178.] Dashboard Definition & Meaning. (n.d.). Dictionary.com. Retrieved February 16, 2022, from https://www.dictionary.com/browse/dashboard

[179.] Raschke, P., Küpper, A., Drozd, O., & Kirrane, S. (2018, June 9). Designing a GDPR-Compliant and Usable Privacy Dashboard. IFIP Advances in Information and Communication Technology,. Retrieved February 16, 2022, from https://doi.org/10.1007/978-3-319-92925-5_14; View your data on the privacy dashboard. (n.d.). Microsoft Support. Retrieved February 16, 2022, from https://support.microsoft.com/en-us/windows/view-your-data-on-the-privacy-dashboard-03d3e27f-1981-5ˆ4-ba1c-d6b1031ae433

[180.] 2021 Privacy Tech Vendor Report. (n.d.). International Association of Privacy Professionals. Retrieved February 16, 2022, from https://iapp.org/media/pdf/resource_center/2021TechVendorReport.pdf

[181.] Ibid

[182.] Ibid

6. When regulations are clear, and institutions are strong enough to enforce liabilities, solutions must integrate this knowledge to indicate Value-At-Risk (VAR), like how portfolio risk management solutions work.
7. It must not become a quarterly or annual solution, only used as a periodic compliance tool. It must be a continuous real-time solution, given that development practice code and deployment change, multiple times a day, has become the norm.
8. It must integrate with a wide variety of data stores (ingests) and with other existing solutions, including SIEM (Security Information and Event Management) solutions.

Having a technical solution is not good enough to ensure privacy outcomes for users. Ultimately, no technology or technical solution operates in a vacuum. Instead, they operate in a space that reflects the internal contestations of engineers, privacy professionals, lawyers, marketing professionals, management and, to a smaller extent, user expectations in interpreting the law. Usually, there is no counterbalancing force to reduce risk accumulation on the liability side, like how financial institutions have a risk and compliance officer with a reporting line, different from the business heads and other revenue generation verticals.

This internal bureaucracy and its capability to enforce privacy-safe practices depend not only on the budgetary allocations but also on the power structures within the organisation and how these competing interests are balanced by a set of arbiters. The resolution of these conflicts, further creates feedback loops, that either amplify or attenuate not just the enforcement processes but also liability estimation. In order to establish a privacy culture within organisations, a holistic way of analysing and doing things is required, which begins with a privacy office that is autonomous by budget and functions.

The positive externality of a privacy-safe culture is sustainability, where risks are mitigated by continuous integration of best practices across the spectrum of data collection, and processing which also does not impede value generation, thus becoming an intangible asset on the balance sheet, in the form of goodwill.

The credibility of goodwill depends on user trust, and hence is not just a function of the claims made by the organisation but is wrapped within the ecosystem of policy, regulations, and enforcement capability. Suppose privacy engineering processes are open to the public (through regulatory mechanisms) – in that case, it can be tested for effectiveness, and the interpretative process of the law through technological solutions can build user trust.

Hence, the data balance sheet approach is both organisation-specific and ecosystem-specific. Just like how a sound balance sheet ensures business expansion across different verticals and geographies, a sound data balance sheet enables expansion without a corresponding increase in liabilities.

Privacy engineering best practices must hence be looked upon not just to reduce liabilities, but to enable responsible and sustainable business expansion, by maintaining a clean balance sheet from both cyber security and privacy angles.

7.2 TECHNICAL STRATEGY

The balance sheet approach allows the creation of a technical strategy that is aligned with a business' way of looking at privacy engineering. For instance, the categorisation of data as both an asset and a liability with expenses incurred to reduce the liability and increase the asset value creates the natural process of:

1. Asset and liability enumeration.
2. Flow mapping of assets and liabilities as where they have been acquired from, and where they are being sent across (ingress and egress of data).
3. Asset and liability categorisation and attaching monetary values to them. Protection measures via risk management practices where assets do not lose value and liabilities do not increase in value.

When applied to the problem of managing data, these processes map into a technical strategy of:

1. Data enumeration (Where and what is the data?)
2. Data flow mapping (Where has it been acquired from, and who has it been shared with and how?)
3. Data categorisation (Where data is labelled as required by legal or other regimes as sensitive, non-sensitive etc.?)
4. Data access control (Where control on who gets access to data is determined by categorisation?)

7.2.1 Data Enumeration

Data enumeration is, first and foremost, an audit process. Like stock audits are conducted, in this step, the entire set of data that the organisation has, is mapped out. While smaller organisations may think of this as a Single SQL database, this view often misses out on the impact of data on supply chains.

For instance, a typical business may subscribe to any number of digital services or other partners including payroll services, payment services, sales tools, communication tools, and marketing services, etc. Every one of these services has access to organisation data to fulfil their contractual obligations.

Further, employees and other support organisations may also collect data and may store parts of it in their devices. This could be either raw data, processed data or even code. With the increasing use of AI/ML, the differentiation between code and data has become less clear, and there have been cases where data was recovered from an ML model via techniques such as Model Inversion.[183]

[183] Wang, Q., & Kurz, D. (2021, November 5). [2111.03702] Reconstructing Training Data from Diverse ML Models by Ensemble Inversion. arXiv. Retrieved February 16, 2022, from https://arxiv.org/abs/2111.03702

Cloud-based data stores (Red Shift,[184] Snowflake[185] etc.) make it very easy to spin up additional nodes for data processing, thus making the data sprawl problem much worse. Larger organisations may have multiple departments that become much harder to manage. They may use a multiplicity of technologies and data storage solutions[186] for quick access to data to run sales and marketing campaigns.

Organisation-wide network scanning tools would help identify these data sources (hosted either in the cloud or on-premises), followed by manual investigation, to create an internal data infrastructure map. Cloud providers, however, allow automatic discovery of new data sources and other resources via configuration services (e.g. AWS Configuration service,[187] Azure Activity[188] Log etc.), thus making it easier for born-in-the-cloud organisations to keep a tab of their digital assets.

7.2.2 Data Flow Mapping

Like how cash flows across various heads and departments, which has an impact on the way in which the organisation functions, the path through which the data flows through the organisation, also has an impact on how privacy is engineered. Flow mapping has two intrinsic components:

1. Ingress and
2. Egress.

For instance, consider the example of a hypothetical organisation that collects data for providing financial services such as home loans.

The flow of data not only indicates data acquisition but also data egress to other entities and points out how additional data sets can be built by interacting with these entities. Flows, hence, can be represented as graphs and loops in the graphs to represent data enrichment via these flows. Egress flows also allow audits to understand:

1. If these flows are already known or are a surprise.
2. Flows are covered by legal agreements on data sharing with these entities.
3. Rights and obligations of data with these entities, which cover storage, processing, retention, and other such restrictions.

Data flow mapping not only covers external data flows but also within various departments of the organisation. The technical architecture that allows flows is typically referred to as Pub-Sub (Publisher–Subscriber) model, where publishers typically put out data that they

[184] Cloud Data Warehouse – Amazon Redshift – Amazon Web Services. (n.d.). Amazon AWS. Retrieved February 16, 2022, from https://aws.amazon.com/redshift/

[185] (n.d.). Snowflake Data Cloud | Enable the Most Critical Workloads. Retrieved February 16, 2022, from https://www.snowflake.com/

[186] Evans, W. (2021, November 18). Amazon's Dark Secret: It Has Failed to Protect Your Data. WIRED. Retrieved February 16, 2022, from https://www.wired.com/story/amazon-failed-to-protect-your-data-investigation/

[187] Supported Resource Types - AWS Config. (n.d.). AWS Documentation. Retrieved February 16, 2022, from https://docs.aws.amazon.com/config/latest/developerguide/resource-config-reference.html

[188] Azure Activity log - Azure Monitor. (2022, February 1). Microsoft Docs. Retrieved February 16, 2022, from https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/activity-log

want to share in an event stream or a data bus, and subscribers who want access to data, subscribe to the stream. Cloud Services support several implementations of Pub-Sub including message queues, webhooks, data streams, etc., for a wide variety of data sources.

7.2.3 Data Categorisation

Categorisation is a labelling exercise, where every piece of data is labelled based on impact on privacy. While it is much easier to start off with labelling well-known items, such as ID card numbers, Bank accounts, Credit/Debit card numbers, Biometric identifiers, etc., privacy engineering is a lot harder to tackle at scale, because of the emergence of clustering effects and context sensitivity.

For instance, consider a hypothetical example of a service that offers protection against automated robot-caller spam. It offers an application that needs to be installed on the phone of any user and needs access to call records and contact information. Consider two records as shown below:

1. Contact Name: XYZ Hospital, Phone number: +91 12345 67890
2. Activity Record: Called XYZ Hospital, Date: MM-DD-YYYY, From Phone: +91 2222 22222.

While the individual labelling of these fields such as the contact name, and phone number from the phone could be marked as PII and not sensitive, when clustered together and stored as activity records, the categorisation would not be accurate and could be sensitive. Further, if XYZ hospital specialises in a particular stream (say fertility or sex change), the frequency and duration of activity records, if clustered together, should be categorised as highly sensitive, as the privacy harm is much higher.

Hence, static data categorisation rules will not work and there is a need for dynamic data categorisation. Categorisation also should spawn across multiple data stores, if data is spread across different databases, while also taking into consideration the clustering effect.

Data categorisation and clustering hence are best handled by AI/ML tools, as it allows models to be built and deployed across different business verticals/sectors, and for specific jurisdictions, with feedback from real-world harms. This approach also allows data processors to implement 'sensitivity-annotation' while servicing data requests from users.

The end goal of the categorisation exercise would be to create an organisation-wide meta-data scheme that not only has the type of information (Credit Card, ID Card#, etc.), but also contains a list of categorisations that is applicable for the data type across various contexts, as shown in the example indicated below (indicative only):

Table 7: Indicative List of Data Categorisation

Field	Storage Type	Sensitivity Types
ID Card Type	STRING	PII, Sensitive
ID Card Number	STRING, NUMBER	PII, Sensitive

Bank Name	STRING	Financial, Sensitive
Bank Account#	STRING, NUMBER	Financial, Sensitive
Credit Card#	NUMBER	Financial, PII, Sensitive
Gender	SELECTION	PII
Address	MULTI-LINE STRING	PII (When clustered)
Email ID	STRING	Sensitive (When clustered)
Phone#	STRING	PII
Purchase Data	TABLE (SKU, QUANTITY, DATE, PRICE)	Sensitive, PII (When clustered)

7.2.4 Data Access Control

Data Access Control refers to various techniques used to restrict fields that were discovered in the previous stages to both internal organisations and external entities. The techniques could be any of the following (non-exhaustive) and could vary based on who gets access:

- **Encryption –** The field is encrypted via any known encryption algorithm, selected based on the Privacy guarantee needed. A key problem that arises in this approach is, where to store the encryption/decryption keys and if a copy of the plain text must be stored elsewhere for regulatory reasons and how to secure access to that data repository.
- **Masking –** Not all aspects of the data is revealed, but only portions of it are shown, using a masking algorithm. These algorithms could be chosen based on the field type and the privacy guarantee.
- **Randomisation –** The field values can be randomised by combining a random value with the actual value. For example, a location field can be randomised by shifting the latitude, longitude value by a randomly generated latitude, and longitude value.
- **Lossy Compression –** Similar to a reducing fidelity of a photo or video, even normal fields like dates and activity records, can be compressed to reduce full fidelity. For instance, a date field can be converted into a year or age field, email address can be replaced with a domain name and so on.
  No Access – A much simpler approach where the entire field is not shared in any form.

A key concern that arises while implementing encryption and masking solutions, is the management of encryption keys and plain text data. These concerns are managed by the emergence of secure computing solutions such as enclaves, vaulting solutions (both hardware and software based). Enclaves operate by using the principle of separation of concerns, where the plain-text data never leaves the enclave once it is submitted and only supports decryption under exceptional circumstances enforced by stricter access control.

Cloud providers support ready-made enclave solutions (AWS,[189] Azure,[190] Google[191]) in various forms, apart from readily available open-source solutions (Vault)[192].

The primary outcome that needs to be achieved at the data access control stage, is an organisation-wide meta-data scheme that outlines the various data types and the access control that is applicable for each one of them for every internal and external entity that has access to it as shown below (indicative only).

Table 8: Indicative Mapping of Access Control

Field	Sensitivity Types	Access Control (Internal Entity 1)	Access Control (Internal Entity 2)	Access Control (External Entity 1)
ID Card Type	PII, Sensitive	As is	As is	Randomisation
ID Card Number	PII, Sensitive	Masked	Masked	Randomisation
Bank Name	Financial, Sensitive	As is	As is	No Access
Bank Account#	Financial, Sensitive	Masked	Masked	No Access
Credit Card#	Financial, PII, Sensitive	Masked + Encrypted	Masked	Masked + Randomisation
Gender	PII	As is	As is	No Access
Address	PII (When Clustered)	As is	As is	Lossy (Only ZIP Codes)
Email ID	Sensitive (When clustered)	Masked	Masked	Masked
Phone#	PII	Masked	Masked	No Access
Purchase Data	Sensitive (When clustered)	Lossy	Lossy	Lossy + Randomization

[189] AWS Nitro Enclaves. (n.d.). AWS. Retrieved February 16, 2022, from https://aws.amazon.com/ec2/nitro/nitro-enclaves/

[190] Build with SGX enclaves - Azure Virtual Machines. (2021, November 11). Microsoft Docs. Retrieved February 16, 2022, from https://docs.microsoft.com/en-us/azure/confidential-computing/confidential-computing-enclaves

[191] Introducing Google Cloud Confidential Computing with Confidential VMs. (2020, July 14). Google Cloud. Retrieved February 16, 2022, from https://cloud.google.com/blog/products/identity-security/introducing-google-cloud-confidential-computing-with-confidential-vms

[192] (n.d.). Vault by HashiCorp. Retrieved February 16, 2022, from https://www.vaultproject.io/

BOX 4

Lossy Compression

It is an algorithm used to reduce the file size of any image by discarding some non-critical information. One such privacy- tech in the market is the attribute-based credentials solution (discussed in our PET chapter. Using this solution, the data principals can reveal only a relevant attribute of personal information for authentication. For instance, if age verification is mandatory for specific authentication, using this solution, data principals can verify their age by inference without disclosing the date of birth.

7.2.5 Data Convergence

Privacy engineering inevitably results in data convergence and the emergence of centralised data lake architecture[193] when carried out over time because of the organisation-wide meta-data schema approach. However, this does not mean that all data must be stored in a single data lake, as the meta-data schema approach encourages library and SDK development to implement access layers.

In programming parlance, these developments are referred to as crosscutting concerns and are typically handled via annotations (where functions that implement access are annotated with other functions that can transform data transparently). Convergence via libraries and SDKs along with meta-data schemas allow internal queries submitted by users such as:

1. What data do you have about me?
2. What data did you share about me with whom?
3. How did you share this data (in what format)?
4. How long have you been sharing this data?
5. Can you delete all data you have on me (OR) a subset of this, and if not, why?

The data convergence approach via the four-step process of enumeration, flow management, classification and access control thus points out how an organisation's privacy engineering practice has evolved. While putting out consent practices, fair practice code, etc., is an important aspect of privacy preparedness, the availability of internal technical practice points are a useful indicator of how effective these practices are. The availability of information about internal practices may be difficult to obtain for third parties in the current scenario. As the data protection regime matures with an increase in privacy engineering, regulators, users, and civil society observers can come up with appropriate confidentiality agreements in place that can enable the scaling up of the industry.

[193] This allows storage of all data (structured/unstructured) at any scale. Analysis or any subsequent action in the data lifecycle can be conducted using data from these lakes.

CONCLUSION

Privacy technology in India is still nascent. It is gradually evolving. However, as discussed in this report, privacy technology in India has been subjected to structural and operational challenges like the lack of privacy-first culture amongst the data fiduciaries, low demand from individuals, budgetary constraints, information asymmetry, etc.

We believe the strategies suggested in this report would help in dealing with the challenges of privacy technology and developing a privacy-first culture in India. Data fiduciaries have already recognised the competitive advantage gained by providing their customer's products and services with in-built privacy measures. In the long term, we envision that the market and technologies evolve in order to not only set a standard for privacy but also help build an industry-wide taxonomy. This will allow technology-based solutions to become an integral element of businesses, which could eventually be used as a strategy to build trust and attract end-users.

The objective of this report is to initiate a conversation on the state of privacy technologies in India and kindle future research on the market readiness of these technologies by developing a standard methodology for testing solutions at large. This needs to include a critical analysis of the kind of feedback mechanisms employed, and the contextual usage of technology tools.

AUTHORS

KAMESH SHEKAR

(Programme Manager - Privacy and Data Governance)

His area of research covers informational privacy, surveillance technology, intermediary liability, safe harbour, issue of mis/disinformation on social media, AI governance etc. Prior to this, Kamesh has worked as a communication associate at Dvara Research. Kamesh holds a PGP in Public Policy from Takshashila Institution and holds an MA in media and cultural studies and a BA in social sciences from the Tata Institute of Social Sciences.

KAZIM RIZVI

(Founding Director – The Dialogue)

Kazim Rizvi is a policy entrepreneur and Founding Director of The Dialogue. He is a lawyer by profession and previous to starting The Dialogue, he worked with the British High Commission. A widely published columnist, he writes regularly on the intersection of technology, public policy and politics and is frequently sought after as a commentator on television.

SREYAN CHATTERJEE

(Research Consultant)

Sreyan Chatterjee is a lawyer by training, having received his degree from the West Bengal National University of Juridical Sciences. He has experience both in the industry as well as in the policy research space across a range of practice areas: finance, technology, mass-media, agriculture and labour policy. His primary area of expertise lies in exploring the linkages between finance and technological transformations of working conditions in various sectors of the economy.

ESHANI VAIDYA

(Researcher)

Eshani Vaidya has a degree in Law and Humanities from Christ University, Bangalore. Her research interest includes privacy, technology, and intellectual property rights. Currently she works on diverse set of technology policy issues and is particularly interested in data governance and digital inclusivity.

SAKSHAM MALIK

(Programme Manager- Competition Law and Policy)

Saksham Malik graduated from Rajiv Gandhi National University of Law, Punjab in 2020 following which he worked in the antitrust law team of a tiered law firm. His work in the policy sphere revolves around interdisciplinary research in the areas of competition law, technology laws and human rights laws. He is focused on employing tools of policy-making, legal aid, advocacy and capacity building to advance the cause of social justice.

KARTHIK VENKATESH

(Researcher)

Karthik Venkatesh is a lawyer by training who is working on copyright and IPR issues with data sharing in the digital economy, impact assessment of regulations relating to personal and non-personal data flows on startup ecosystems, and the future of a sharing economy

SOUMIL GUPTA

Investment Specialist, Invest India

In his current role at Invest India, Soumil specializes in areas of Information Technology and Renewable Energy, working closely with the industry and the government to facilitate the growth of these sectors. Previously, he worked at the Strategy and Operations team at Zomato after completing his Engineering from BITS Pilani.

SIMRAN KHURANA

Senior Investment Specialist, Invest India

Simran leads the Technology team at Invest India, the National Investment Promotion & Facilitation Agency of the Government of India. Her expertise lies in supporting global MNCs in their India expansion operations, focusing on businesses in the IT and emerging tech sectors. In addition to grounding global investments across GCC and Data Centre majors, Simran actively collaborates with the Ministry of Electronics & IT and various State Governments on policy initiatives and projects to deepen the ITBPM ecosystem in the country.

Simran completed her bachelor's in accounting and finance from Jai Hind College, Mumbai where she also attained her post- graduate degree. Alongside college, she has completed all 3 levels of CFA exam with her charter pending.

@_DialogueIndia

https://www.linkedin.com/company/the-dialogue-india

@thedialogue_official

https://www.facebook.com/TheDialogueIndia

@investindia

https://www.linkedin.com/company/invest-india/

@investindiaofficial

https://www.facebook.com/InvestIndiaIPA/