konnektiv

AI - Privacy Conundrum

A Comparative Study of AI National Strategies and Data Privacy Regulations in Germany and India

Sreekanth Mukku

August 2019

This paper is produced for Konnektiv summarized from the master thesis submitted to the Willy Brandt School of Public Policy on 11 July 2019.

Introduction

This research has explored two inter-related raging debates of recent times surrounding: AI and data privacy: a) debates around data privacy and its breach in an era of digitalization and, b) harnessing of artificial intelligence for growth and technological innovation. Combining these two, this study is primarily concerned with the issue of how data privacy is approached in the artificial intelligence (AI) national policy making for technological advancement. AI has been hailed as a beneficial technology if responsibly deployed to learn from Big Data[1] and help in decision making. It is estimated that AI powered applications in different sectors could contribute 14 percent growth to economic output of the world by 2030[2]. AI based applications have the potential to realize a better and more efficient public sector, new methods of climate and environmental protection, a safer society, and perhaps even a cure for cancer[3]. Conversely, implementation of AI for surveillance, face detection and social media intelligence (among other things), raises major privacy implications for individuals. Machine learning necessitates collection of personal data of users to train the algorithms. Evidence of data privacy breach is prevalent due to the AI enabled developments. Instances of data being not used for intended purposes – data misuse and data persistence are concerns that national strategies have grappled with. Tech firms and government agencies collect personal data of individuals and process this data without the knowledge of the users. For example, algorithmic calculation provides product suggestions for those surfing the web, or tailor news to those browsing feeds on their social media accounts, or even does data combing for targeted advertisements. The tech giants' reliance on Big Data to attract advertising revenue and improve their products has also sparked concerns about user privacy and forced countries to pass laws protecting it[4]. Facebook CEO Mark Zuckerberg appearing before Congress regarding a data mining scandal in Cambridge Analytica's case (Stoycheff 2016), which forced Facebook to revise how data is handled. Other examples include Yahoo! Inc., owned by telecom giant Verizon, which came under juridical radar in 2018 for its practice of combing users' email accounts for data for the potential benefit of advertisers[5]. Moreover, opaqueness of algorithmic functioning and absence of explainable AI makes the understanding of privacy even more difficult.

Given this backdrop, this study asks: how are data protection and privacy concerns addressed in the Artificial Intelligence national strategies of Germany and India? As a comparative public

[1] According to ico.org.uk - Big Data usually refers to massive volumes of data, collected from multiple sources, mostly in real time (See https://ico.org.uk/for-organisations/guide-to-data-protection/big-data/)
[2] See https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf
[3] See Artificial Intelligence and Privacy. Datatilsynet, A Norwegian Data Protection Authority (January 2018).
[4] See https://www.nytimes.com/2019/06/03/opinion/google-facebook-data-privacy.html
[5] https://www.wsj.com/articles/yahoo-bucking-industry-scans-emails-for-data-to-sell-advertisers-1535466959

policy study, taking these two countries as case studies, the research also seeks to know the ways in which both countries' AI policies converge or diverge in its approach to data privacy. The rationale behind choosing these two countries are based on a few commonalities shared by them – both are functioning democracies where right to privacy is upheld by law, both have a federal system of governance and more importantly both the countries came out with their respective AI policy in 2018. Yet, by taking a country from global north and one from global south, the comparison of both countries' AI policy strategy holds the promise of understanding the value each attach to privacy concerns. Looking at cultural and economic logics of these two countries, the study further asks: what are the emergent data protection and privacy concerns that national Artificial Intelligence strategies could pose in either of these countries? Moreover, are privacy concerns overridden by the logic of innovation and job creation in AI policy making? If so, in which ways?

The answers to these questions are looked for in relevant literature. First, borrowing from Hofstede's Cultural Dimensions Theory[6], this study explores the Individualism Vs Collectivism framework to understand how policy making can differ owing to national cultural variations. Following Hofstede's conception - India as a society tends more towards collectivistic culture whereas Germany is an individualistic society[7]. Second, AI – Privacy conundrum is addressed through the issue of privacy guaranteed constitutionally as individual right, choice and freedom that are respected in different democratic countries despite cultural differences. Right to privacy is implicitly enshrined in the constitutions of both Germany and India through different provisions. This fundamental right remains unchanged despite the growing popularity of the idea that AI is a transformative technology that can promote collective benefit. Framing the study around these two concepts, the study does an in-depth analysis of German and Indian AI policies from a comparative perspective. The findings of the study aim to provide recommendations for policy makers dealing with AI and data privacy. At present, there is no available literature which has delved in to AI national strategies from the privacy perspective that deals with two different country cases, one from global north and the other from global south. This study therefore attempts to fill an important lacuna in AI policy study.

[6] Miltgen, C. L., & Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns: a qualitative study in seven European countries. *European Journal of Information Systems*, *23*(2), 103-125.
[7] https://www.hofstede-insights.com/country-comparison/germany,india/

Germany's AI National Strategy – "AI Made in Germany"

According to the German AI national strategy document[8], Germany's Federal Government launched its national Artificial Intelligence (AI) strategy in November 2018. The strategy was developed by the Federal Ministry of Education and Research, the Federal Ministry of Labor and Social Affairs based on the suggestions taken from the nationwide consultations. Germany has allocated an initial budget of €500 million to implement its AI strategy and plan to increase this budget to €3 billion by 2025. With this strategy in place Germany plans to provide a concerted policy response to the rapid advances taking place in the field of AI. The AI strategy has outlined the following three major goals:

1. To make Germany and Europe a leading center for AI and by doing so, it plans to secure Germany's competitiveness.
2. To develop responsible AI and use AI for the good of society
3. To integrate AI in society in ethical, legal, cultural and institutional terms in the context of a broad societal dialogue and active political measures

By setting the above goals, Germany emphasizes on achieving both economic goals and societal goals and seeks to leverage AI for all policy areas within the democratic principles and framework. The national AI strategy recognizes AI as a fundamental innovation which has potential to create both opportunities and risks for the public sector, society, business, administration and science. According to a study commissioned by the German Federal Ministry for Economic Affairs and Energy, AI technology could add €32 billions to the country's manufacturing output over the next five years. Germany recognizes its challenges in adopting to the AI paradigm, particularly in the commercial segments barring manufacturing sector where it has a leading position and outlined "*Industrie 4.0*"[9] strategy to keep up its competitive advantage by deploying digital technologies and automation including AI technologies[10].

The national strategy opines that some of the large German enterprises have been responding well to the AI shift, however, for small and medium enterprises (SMEs or Mittlestand) adoption of AI technologies has been slow as they face challenges in technology transfer and resources to build AI systems all by themselves. To mitigate this challenge the strategy document outlines a targeted Mittlestand 4.0 strategy to increase AI support for SMEs and set up The Mittelstand 4.0 center of excellence to train 1000 companies in AI per year. The document also lays strong emphasis on AI research, skill development to face the structural changes that the labor market

[8] See https://www.ki-strategie-deutschland.de/home.html, English version of the document can be downloaded from the site

[9] INDUSTRIE 4.0 is the name given to the German strategic initiative to establish Germany as a lead market and provider of advanced manufacturing solutions.

[10] https://www.gtai.de/GTAI/Navigation/EN/Invest/Industries/Industrie-4-0/Industrie-4-0/industrie-4-0-what-is-it.html

will undergo due to the AI deployment across sectors. The AI strategy also focuses on supporting AI based startups with funding opportunities and other resources. The federal government's digital hub initiative plans support startups to be more AI savvy. The strategy also outlines number of initiatives like: digitalization of education, imparting AI skills from the school level itself, adopting AI and Big Data technologies in the healthcare sector while complying with data protection rules, deploying AI for safer, environment friendly, more efficient and affordable transportation and using AI for government administrative tasks. Apart from these initiatives, the strategy also has keen focus on involving different stakeholders like business, civil society and research communities in data governance process.

German AI national strategy has envisaged a comprehensive human centric ethical and regulatory framework that would protect the rights of individuals including the right to privacy within the AI enabled environment. The strategy further lays focus on "protecting democratic order and the fundamental rights enshrined in the constitution with particular mentioning of the protection of privacy and control of individual's personal data"[11]. To reap benefits of AI, algorithms require high quality data sets to produce desired results, in this process where personal data is used, the entities that process the data needs to comply with the legal requirements. The EU General Data Protection Regulation (GDPR)[12] provides high data protection standards to protect right to personal data within the EU. The ethical framework developed at the EU level will be adopted and the German government promotes "ethics by, in, for design" approach for AI use.

Germany's national strategy is ambitious in its approach to deal with data privacy concerns that arise in AI enabled environment, however it suggests that it is exploring ways to harness the prowess of AI while not undermining the fundamental rights of individual privacy and democratic values. The Federal government is planning to commit funding for the development of applications that promote privacy of citizens there by providing skills to use AI enabled products and services. The measures to protect and promote right to privacy also include ensuring all sections of population have gained a satisfactory level of confidence in AI based products and services and equip the professionals and administrative functionaries with skills required to verify and review the functioning of AI systems. The strategy further seeks to collaborate with other EU countries and international players to set the global technological standards to reduce barriers and to open markets. Thus, the German government seeks to engage with the private sector, civil society and international community to develop responsible

[11] See page 37 in https://www.ki-strategie-deutschland.de/home.html, English version of the document can be downloaded from the site

[12] See https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

AI that works for good of the society, even as it aims to promote economic growth and innovation.

Experts working on German AI strategy and data privacy opine[13] that the country has adequate legal and regulatory protection against any privacy violations of personal data belonging to the individuals. Nevertheless, AI enabled economic structure poses potential challenges for regulators to determine with whom the data ownership lies. Functioning of current AI systems rely on big data, social media data and personalized data, to train their algorithms for companies to operate in the automated outcomes. There are three sets of commercial enterprises which are primary AI players - social media and general internet platforms (e.g. Facebook, Google and Twitter), ecommerce companies (e.g. Amazon and Zalando) and industrial AI/automation companies (e.g. SAP, Bosch and Siemens). Given Germany's focus on industrial AI, big companies would own the platforms and sell their AI products and services to the third-party enterprises (e.g. BMW and Volkswagen). In order to improve efficiency and productivity to benefit consumers these AI platforms capture data to train their algorithms. The data sharing between the companies raise a pertinent question - who owns the data and how can the legal system put onus of data ownership and responsibility? The data captured by social media and ecommerce companies is a bigger political question as the data is personal data of the individual users, whereas in the industrial AI environment the data is related to trade secrets and the data ownership is a question of competitive landscape. The power of the AI platform and ownership of data could potentially lead to power struggle among the big players and this powerful dominant position of the market winners could also mean that 'winner takes it all' like big tech firms in the social media and ecommerce sectors. There is also danger that the winner could set the technical standards for others to follow. However, the ecosystem could prevent such danger as other stakeholders within the ecosystem have to cooperate with each other for data sharing in industrial AI sphere. Both the market mechanism in AI ecosystem and regulatory mechanism in Germany and EU will not allow monopolies to grow and violate fundamental right to privacy of personal data. As one expert and a member of Enquete Commission established by German Bundestag, Whom I interviewed in June 2019 said:

> *The German national AI strategy says 'AI made in Germany', but it's an anachronism, as AI is an international technology and Germany's presence in global social media, ecommerce and infrastructure market is limited which makes Germany vulnerable from national security standpoint.*

[13] This sub section is based on the interviews conducted with AI and Privacy experts from Enquete Commission of the German Bundestag on "Artificial Intelligence – Social Responsibility and Economic, Social and Ecological Potentials"WZB and Weizenbaum Institute

Another expert who is a researcher in a Berlin based think tank also suggested something similar during an interview conducted in May 2019 said:

> *There is no evidence to suggest that tighter privacy regulations could slow down innovation, we need to reflect on this discourse because this line of argument would be good for entities that rely on data capture and put efforts to weaken regulations that protect citizens' privacy.*

To ensure responsible AI adoption and to derive competitive advantage, Germany is investing in technologies which comply with regulations and standards that make AI activity ethical and responsible. German enterprises are expected to build *privacy by design*[14] in to their products and services. Therefore, Germany would not follow lighter regulatory framework that is prevailing in the USA nor would it follow tighter state control model practiced in China. Germany wants to articulate its strategy – while playing to its strengths in manufacturing and industrial AI at the same time to promote ethical AI products and services to its competitive advantage. It sees this strategy as an integral part of EU strategy rather than a standalone German AI national strategy, yet it seeks to give its AI game a distinctive German identity.

India's AI National Strategy – "AI for All"

India has outlined its national AI strategy in June 2018 in a discussion paper published by the National Institution for Transforming India[15] (NITI Aayog), a think tank set up by the government of India. NITI Aayog has developed AI strategy[16] in collaboration with *Digital India* (India's national digital initiative) and the Ministry of Electronics and Information Technology and has set up five-member expert committee with a budget allocation of €426 million (NASSCOM, 2018)[17]. The strategy document identified five sectors as key priority areas where AI technologies will be leveraged, they are: Healthcare, Agriculture, Education, Smart Cities and Infrastructure, Smart Mobility and Transportation. India's AI strategy revolves around three major themes which are to fulfil its economic and social development goals: 1) Tapping into potential economic opportunity by leveraging AI; 2) realizing social development and inclusive growth; 3) Making India AI solutions hub and provider of choice for the emerging and developing economies (excluding China) (Niti Aayog, 2018).

The strategy believes that AI will bring transformative development to the large population of India and seeks to make AI as an agent of future economic development of the country. Indian

[14] See https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf
[15] See https://www.niti.gov.in/content/overview
[16] See https://niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf
[17] See https://www.nasscom.in/system/files/secure-pdf/NASSCOM_AI_Primer_2018_11072018.pdf

government plans to leverage AI for strengthening public delivery system which is marred by inefficiencies. The government sees the promise in AI technologies like Big Data, Analytics and IoT based systems to improve planning, execution and monitoring of public services like education, health, transportation, etc. The strategy lays emphasis on making India a hub of AI solutions and plans to provide AI solutions to the emerging economies across the world. Overall India's AI national strategy identified five major sectors where AI will play a defining role to transform these sectors:

1. To build quality education system with help of AI and building AI talent pool
2. To improve overall health outcomes by creating electronic repositories for healthcare data for machine learning and develop national scale clinical decision support system
3. To drive new agriculture revolution to meet increasing demand
4. To improve urban infrastructure, public safety and create smart cities
5. To create intelligent transportation system to reduce accidents and improve traffic flows

According to an Accenture report published in 2017[18], AI has potential to add US$ 957 billion or 15 percent of gross value addition to India's economy in 2035. Niti Aayog also proposed the following measures in line with the national strategy: 1) €970 million investment plan for creating an national AI institutional framework which will be used to set of research centers and oversee implementation of national AI strategy; 2) Plan to develop an AI readiness index that will rank states on their AI adoption capabilities[19].

The strategy document's vision for AI to tackle public safety and crime contradicts with the protection of data privacy goals outlined. On the one hand the document explains the privacy concerns and how personal data of the citizens is to be protected, on the other hand it lays out adoption of sophisticated surveillance systems and use of social media platforms to monitor people's movement to maintain public safety. Both are inherently contradicting. The government's proposal to implement surveillance systems conflict with the forthcoming personal data protection bill[20] (which is expected to be tabled in the parliament) and recent Supreme Court rulings[21] on right to privacy. The document recognizes the privacy rights of consumers and need for regulation of capturing, processing and inappropriate use, discrimination and so on, but fails to underscore the role of the government in data governance and remedy and redressal mechanism if government is the offender and violated data privacy

[18] See https://www.accenture.com/us-en/insights/artificial-intelligence/technology-revolution-like-no-other
[19] See https://economictimes.indiatimes.com/tech/internet/niti-aayog-plans-index-to-rank-states-on-artificial-intelligence-adoption/articleshow/69570190.cms?from=mdr
[20] See https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf
[21] See https://privacyinternational.org/state-privacy/1002/state-privacy-india

of individuals. One Indian respondent, founder of a civic tech company in India, Whom I interviewed in June 2019, explained this conundrum:

> *Government treats personal data of citizens as public data and sees its role as a custodian of the data there by it can have absolute rights over the citizens data in the larger public interest, particularly in the interest of national security and development.*

Another respondent (interviewed in July 2019) who works as a vice president for Big Data and AI in a startup operating in AI technology put India's privacy concern in perspective and pointed out:

> *AI cannot be just used for generating ad revenue by capturing personal data of people, it's a powerful technology that can be used to solve both business and social problems especially in a country like India. But India has to have tighter regulations to protect citizens privacy and provide confidence to the people in AI technologies then only its potential can be realized.*

India's low literacy levels and inadequate awareness of data privacy on digital platforms will make the law enforcement extremely complex and a difficult proposition. The opacity of AI functions and the absence of explainable AI would also make even literate population vulnerable to data privacy threats. India's diverse demographics also pose a challenge for government to conduct mass awareness programs with limited resources at its disposal. A case in point is the recent government drive for financial inclusion by opening bank accounts for unbanked population and linking them to bio metrics enabled unique identification number (Aadhaar)[22] that stores personal data of the citizens[23]. The majority of the beneficiaries of these bank accounts come from socially and economically backward communities and have limited literacy levels and digital knowhow to understand the vulnerability of their data privacy which is in the hands of not only government but also with other financial institutions. This section of population which is increasingly interacting with the digital ecosystem possibly has limited awareness of the recent Supreme Court judgement that proclaimed privacy as a fundamental right (CIS-India, 2018[24]).

It is important to understand the new privacy bill in detail, which is prepared to be legislated by the government of India, to assess its strength to protect data privacy of citizens at a time when the big data-AI will have political and socioeconomic implications. The Government of India started the process of drafting and enacting the data protection bill in 2010 to deal with the privacy violation concerns arising in the data driven environment fueled by increasing internet

[22] Aadhaar issued by government of India to eliminate duplicate and fake identities, and to verify and authenticate in an easy, cost-effective way

[23] See https://uidai.gov.in/about-uidai/unique-identification-authority-of-india/about.html

[24] See https://cis-india.org/internet-governance/blog/the-srikrishna-committee-data-protection-bill-and-artificial-intelligence-in-india

and smartphone penetration. The right to privacy has become one of the key policy debates in India following the implementation of Aadhaar (biometric identification of the citizens). There were cases filed to question the validity of the Aadhaar implementation as it violates fundamental right to privacy of the citizens. The Supreme Court of India ruled that the right to privacy is a fundamental right guaranteed by the constitution of India and Aadhaar cannot be mandatory for citizens to avail any public services. However, the court ruling was criticized by some as it had left a potential loophole where state can violate to protect its legitimate interest[25]. In 2017, the government set up a committee of experts headed by justice Srikrishna (a retired justice of supreme court of India), constituted by Ministry of Electronics and Information Technology. The committee of experts submitted its draft report in July 2018. The draft bill is titled "The Personal Data Protection Bill, 2018". The bill is tabled and expected to come for discussion in the parliament. Though the bill is considered as a right step by the government to deal with data privacy violations there are concerns expressed by various stakeholders, especially civil society organizations.

A recent report by Access Now[26] offers some valid criticism in this regard. The report states that the bill was drafted without wide range of consultations especially the committee did not conduct enough public consultations to include diverse range of perspectives from the large population of India. The consultation and negotiation process during the process of drafting the bill was not transparent enough and the committee did not divulge to the public the outcomes of various consultations it held with different stakeholders. The provisions of the bill which deal with data processing allows state agencies to process citizen data without consent and it gives the state an absolute right over citizen data which is a violation of the fundamental right to privacy of the citizens. The bill provisions also state that the personal data may be processed for "reasonable purposes", which is vague and leaves for variety of interpretations and thereby has potential to violate the privacy of the individual not only by the state but also by private entities for commercial purposes.

The bill provisions apply to the processing of personal data of the individuals which is collected, disclosed, shared, or processed within the Indian territory, it also seeks to enforce data localization by making it mandatory for every data fiduciary to store a copy of the user's personal data on a server or data center located in India. There is an exception created to this rule wherein the central government may make certain categories of personal data exempt from the requirement of local storage on the grounds of strategic interests of the state. This

[25] See https://timesofindia.indiatimes.com/india/supreme-court-verdict-on-right-to-privacy-what-legal-experts-say/articleshow/60218906.cms
[26] See https://www.accessnow.org/cms/assets/uploads/2018/10/Assessing-India%E2%80%99s-proposed-data-protection-framework-oct18.pdf

provision potentially gives more control to the government over personal data of the user and leaves room for the third party to infringe upon the right to privacy of the user. The provisions for cross-border data transfers of non-critical personal data are similar to GDPR. However, the bill does not provide users the right to explanation in automated decision-making environment; this right ensures certain level of accountability and transparency for the users when algorithms are used to make decisions. Though the bill makes provision for right to be forgotten, it does not give the user right to erasure which is an important provision under GDPR. The report opines that the draft bill requires further consultations with wider spectrum of stakeholders in order to improve the key provisions of the bill.

If India wants to harness the full potential of AI technologies and give empower people as envisaged in its national AI strategy, a foolproof data privacy law should be legislated and enforced effectively. In a diverse society like India, strict implementation of such law requires massive amount of resource deployment and capacity building at every level of governance. Yet, this investment is necessary if India is serious about playing a lead role as a hub and an exporter of AI services and products in emerging economies in the global south.

Policy Convergence and Divergence

Based on the insights drawn from the literature, content analysis of AI strategy documents, Hofstede's model, and expert interviews, the analysis below demonstrates how Germany's and India's national AI strategies converge and diverge in the way they deal with the data privacy.

Areas of Convergence

Sl.No	Germany	India
1.	Right to Privacy is a fundamental right guaranteed in the constitution	Right to Privacy is a fundamental right ruled by the Supreme Court of India
2.	Strong emphasis on privacy in National AI Strategy	Moderate emphasis on privacy in National AI Strategy
3.	Private sector largely for not tighter privacy regulations	Private sector not for tighter privacy regulations
4.	Advocates strong global cooperation for AI and Data governance	India moderately in favor of global cooperation on AI governance

Details of privacy areas of convergence between Germany and India

Source: Author

Areas of Divergence

Sl.No	Germany	India
1.	Individualistic society	Collectivistic society
2.	Higher awareness about right to privacy	Low awareness about right to privacy
3.	GDPR is in force – a model for data privacy across the world	Personal Data Protection Bill yet to be legislated
4.	Multi-stakeholder consultation on AI national strategy	No consultation on AI national strategy
5.	AI Startups are geared to adopt GDPR	AI startups are apprehensive about new privacy bill draft
6.	Heavy focus on Industry	More focus on services sector and social sector (Health, Education, Agriculture)

Details of privacy areas of Divergence between Germany and India

Source: Author

Both Germany and India guarantee right to privacy as a fundamental right in their respective constitutions. While Germany has adopted GDPR to protect data privacy of its citizens, India is yet to legislate the personal data protection bill draft which will be tabled in the parliament. India's inadequate resources limited administrative and legal capacities weaken its ability to enforce privacy laws and prevent it to take any actions against violations in a timebound manner. Germany on the other hand is better prepared to deal with any privacy violations effectively. Indian government did not conduct wide range public consultations nor engaged with all the key stakeholders while developing its AI strategy. Germany had a wide range of consultations with all stakeholders to ensure that the strategy is inclusive. The German AI strategy categorically its position on data privacy and how it will take measures to ensure the personal data is protected. Though private sector in genera is not favor of tighter privacy regulations in both the countries, German companies and startups are more inclined to complying with GDPR and see ethical AI could be a potential market opportunity. The research findings from expert interviews reveal that the stakeholders in India are divided on the issue of privacy – Indian government and private sectors see personal data as a monetizable resource and there is a sense that tighter privacy law and its enforcement could obstruct AI lead innovation and growth. However, civil society and intelligentsia of the opinion that growth cannot come at the cost of right to privacy. Germany's AI strategy is heavily focused on manufacturing/industry sector, which would put the private sector in the driver seat to steer the AI agenda rather than government taking the control of agenda-setting and let the private

players develop innovations. This would also mean that the other important sectors such as education and healthcare might not be able to attract adequate AI investments. In India's case, the AI strategy has strong focus on services and social sectors. Interestingly Manufacturing sector doesn't figure among the core five sectors. Thus, India's focus sectors have to draw personal data from the users to train algorithms to obtain desired results. This also enables government to play major role in data governance, where government control over large volumes of personal data might lead to unwarranted surveillance. The new draft data protection bill doesn't address this concern as it gives government power to control and process personal data of the citizens if it involves matters of national interest[27].

Privacy and Innovation/Competitiveness Indicators

Based on research carried out for this study, the report examines key privacy and innovation/competitiveness indicators for both Germany and India. This comparative analysis is drawn to show how they fare on seven such indicators. Each indicator is evaluated based on the ranking or score both the countries obtained in respective indices taken from different sources where the research results were published in the public domain.

Evaluation Indicator	Germany	India
Level of Data Protection[28]	Adequate Country (High)	Existence of certain form of Data Protection Laws (Low to Moderate)
Internet Privacy[29]	High	Low
Government AI readiness Index 2019[30]	Rank: 3	Rank: 17
Automation Readiness 2018[31]	Rank: 2	Rank: 18
Global Innovation Index 2018[32]	Rank: 9	Rank: 57
Global Competitiveness Index 2019[33]	Rank: 3	Rank: 58
Hofstede's Model Individualistic/Collectivistic[34]	Individualistic Society – Individualism Score: 67	Collectivistic Society – Individualism Score: 48

Comparison of key indicators

Source: Author – based on indices extracted from multiple sources

[27] https://www.accessnow.org/cms/assets/uploads/2018/10/Assessing-India%E2%80%99s-proposed-data-protection-framework-oct18.pdf
[28] See https://www.cnil.fr/en/data-protection-around-the-world
[29] See https://bestvpn.org/countries-ranked-by-privacy/
[30] See https://www.oxfordinsights.com/ai-readiness2019
[31] See https://www.automationreadiness.eiu.com/
[32] See https://www.wipo.int/pressroom/en/articles/2018/article_0005.html#rankings
[33] See http://www3.weforum.org/docs/GCR2018/05FullReport/TheGlobalCompetitivenessReport2018.pdf
[34] See https://www.hofstede-insights.com/country-comparison/germany,india/

Germany fares far better on both privacy and innovation/competitiveness indicators. Germany's top position in privacy, AI readiness of the government, automation readiness, innovation and competitiveness indicate that a country can achieve privacy while demonstrating its readiness for AI implementation and remain competitive. The insights from the expert interviews also corroborate to this fact that AI led innovation and data privacy are not mutually exclusive, rather they both are essential for the overall progress of economy and society. It is also to be noted that India as a collectivistic society in Hofstede's framework might value privacy not at individual level but at social groups level[35]. Indian Supreme Court ruled that data privacy is a fundamental right of citizens of India. Culture of privacy is understood and practiced in a local context, but the nature of the data flows and AI technologies operate in international and interconnected environment, therefore data privacy also needs to be contextualized in global context.

After analyzing the various data points from variety of sources this research shows that there is no evidence to suggest that the tighter data privacy regulation could undermine the governments' push for aggressive AI strategy to reap benefits of innovation, job creation and productivity. Therefore, one can argue that the Germany's privacy regulatory framework doesn't impact adversely its push for AI lead innovation, growth and job creation. Thus at this stage there is no evidence to suggest data privacy regulatory norms undermine AI lead innovation and growth. AI's progress in many areas has far reaching adverse implications on individual privacy – it is real, and the evidence is prevalent. Innovation and privacy are not mutually exclusive. Just as how innovation is an engine for growth, privacy is vital for individual well-being – it is their fundamental right. Notwithstanding Hofstede's national cultural model – despite cultural differences in individualistic and collective society – privacy is still valued although it is imagined in different ways. Privacy is an important part of cultural life in collectivist societies too and people are sensitive about it.

Conclusion

The key findings emerging from this study are twofold: first regarding data collection by AI for innovation and growth and second its implication for privacy. Germany and India's recent AI national strategies to harness AI for future innovation and growth opens a window to compare these prospective AI national policies in a comparative framework. The specific aim has been to study convergences and divergences in these national strategies and explore how privacy

[35] Basu, S. (2012). Privacy protection: a tale of two cultures. *Masaryk UJL & Tech.*, *6*, 1.

concerns are handled in these documents given AI's propensity to work with Big Data, much of which relies on personal data.

The comparison of German and Indian AI policy strategies brings out some points of convergences: both countries acknowledge privacy as a fundamental right, and both have made AI development as one of the key policy agendas given its potential to fuel future growth. Germany and India have similar AI enabled growth vision and framed privacy as a fundamental right through their constitutional mechanisms. Yet, there are points of divergences as well. Variations in terms of cultural, political and economic context exist in the way each country views privacy. Germany's privacy laws and enforcement are stronger compared to India's. Germany's AI national strategy emphasizes on strong ethical standards and wish to build competitive advantage around its ethical AI solutions. In India's case, development, growth, job creation, skill development takes precedence over ethics and privacy issues.

Germany's multi-stakeholder approach is contrary to top down push approach of India regarding AI national agenda setting. In German scenario privacy is embedded in German sociocultural life - Germany complies with one of the strict data privacy regulation GDPR despite German industry being one of the early adopters of AI – Industry 4.0. Despite its strict regulation, the country has planned investment in AI is worth €1.5 billion. It also ranks 3rd among the countries on Government AI readiness. On the other hand, India's privacy regulation bill still not legislated, because of which its enforcement is weaker which poses a challenge to privacy concerns. India is a collectivistic society where privacy is dealt differently at individual level, institutional level and social groups level. India ranks 17th on Government AI readiness and to improve it, it also wants to push AI in a big way and has set aside €426 million for its implementation. The gap in budgetary allocation for AI between India and Germany and their positions in AI readiness indicates that India still lags behind in AI adoption. Even though privacy is a concern for India, it may conversely push India to further ignore privacy concerns (increased surveillance and social media monitoring of its citizens) in implementing AI technologies. Germany's AI readiness suggests that there is no conclusive evidence to suggest that AI push will lead to weakening of data privacy.

Recommendations

Based on research conducted for this study, the following policy recommendations are proposed for policy makers in India and Germany.

The following recommendations are made for Indian policy makers:

1. Privacy by Design: Privacy by Design (PbD) (Cavoukian 2009) is developed in recent years as a legal and technological concept that helps enforce data protection obligations and make privacy a priority in an organization. This not only ensures data protection but also leads to data integrity. PbD is one of the key principles of data protection adopted by the EU GDPR.
2. Human in Command Approach: AI should empower humans and AI systems need to work under human oversight to reduce potential risks of data breach and privacy challenges. the development of AI be responsible, safe and useful, where machines remain machines and people retain control over these machines at all times. This approach is part of EU's ethics guidelines for "building trust in human-centric AI" which was unveiled in April 2019.
3. India needs to conduct further public consultations to improve the draft bill in order to keep up to the data privacy challenges posed by the big data-AI ecosystem. Especially, the bill should include the right to explanation and right to erasure.
4. As right privacy is a fundamental right, it is imperative upon the government to make citizens aware of their right to data privacy. The knowledge of the data privacy law provisions in India have to be disseminated to all sections of the society in the local languages and make them easy to comprehend for everyone.

The study also makes following recommendations for policy makers in both India and Germany:

5. Multi-stakeholder global cooperation for AI governance: Multi-stakeholder engagement in setting AI policy agenda will lead to protection of interests (including data privacy) of various social groups. Global cooperation for AI policy formulation, setting technical, ethical and privacy standards in its use and implementation is an imperative. The nature of the data flows are international and AI technological ecosystem operates in an interconnected environment; therefore, data privacy also needs to be contextualized in global context. Thus, it is imperative for all policy makers to push for AI and data governance at international level. Stakeholders also must push for technology transfer and collaborative multidisciplinary research of AI to design privacy regulations and systems.
6. Integrating basics of data privacy and AI ethics into the school curriculum at least in the secondary school will help creating awareness about right to data privacy and the potential violations that could harm the users of data in data-driven environment.