WZB
Berlin Social Science Center

Kim Arora

# Privacy and data protection in India and Germany: A comparative analysis

**Discussion Paper**
SP III 2020–501
January 2020

Research Area
**Digitalization and Societal Transformation**
Research Group
**Politics of Digitalization**

WZB Berlin Social Science Center
Reichpietschufer 50
10785 Berlin
Germany
www.wzb.eu



Kim Arora
**PRIVACY AND DATA PROTECTION IN INDIA AND GERMANY: A COMPARATIVE ANALYSIS**
Discussion Paper SP III 2020–501
Wissenschaftszentrum Berlin für Sozialforschung (2020)

Affiliation of the author

**Kim Arora**
Berlin Social Science Center (WZB)
German Chancellor Fellow 2018-19 supported by the Alexander von Humboldt Foundation

Abstract

## Privacy and data protection in India and Germany: A comparative analysis

by Kim Arora*

This research report offers a comparative analysis of privacy and data protection in Germany and India. It compares the two regimes on four counts. First, it examines how the right to privacy and/or its allied rights have developed in the two countries historically. In this, it explores the political factors contributing to the understanding and acceptability of the principles of privacy in the decades after the Second World War. Second, it delves into the instruments and forms of state surveillance employed by both the countries and analyses how the presence of parliamentary and judicial oversight on intelligence agencies impacts individual privacy. In the third section, it compares how biometric identity systems have been deployed in the two countries, the safeguards designed around the same, and the legal challenges they have thrown up. Lastly, it evaluates data subject rights as defined under the General Data Protection Regulation (GDPR) together with the Bundesdatenschutzgesetz-Neu (BDSG-Neu) and how they compare with those as defined under the Draft Personal Data Protection Bill, 2018 in the Indian context.

*Keywords: data protection, surveillance, biometrics, Internet regulation, comparative analysis, India, Germany*

---

* The author would like to thank the Alexander von Humboldt-Stiftung (AvH Stiftung) and Wissenschaftszentrum Berlin für Sozialforschung (WZB) for their support in carrying out this project. Financial support for this work came in the form of the German Chancellor Fellowship (2018-19) from the AvH Stiftung. The WZB served as the host organisation for the duration of the project and provided institutional and logistical support. The author would like to extend a special thanks to Prof Dr Jeanette Hofmann, head of the research unit Politics of Digitalisation (POLDI) at the WZB, for the opportunity to work with the institute. Gratitude is also due to Dr Julia Pohle, research fellow at the POLDI unit, for her unstinting support, generous guidance, and persistent encouragement.

This report was produced as part of the German Chancellor Fellowship, and completed in November 2019. The version of India's data protection bill referred to here, therefore, is the Draft Personal Data Protection Bill of 2018, as drafted by the B N Srikrishna Committee. This is not a peer-reviewed text.

## Table of contents

## List of abbreviations

| | |
|---|---|
| **AFSC** | Afghanistan SIGINT Coalition |
| **BDSG** | Bundesdatenschutzgesetz |
| **BND** | Bundesnachrichtendienst |
| **BRH** | Bundesrechnungshof |
| **BfDI** | Bundesbeauftragter für den Datenschutz und die Informationsfreiheit |
| **BfV** | Bundesamt für Verfassungsschutz |
| **CBI** | Central Bureau of Investigation |
| **CCC** | Chaos Computer Club |
| **CCPA** | California Consumer Privacy Act |
| **CIDR** | Central Identities Repository |
| **CIS** | Centre for Internet and Society |
| **CMS** | Central Monitoring System |
| **DSPE** | Delhi Special Police Establishment |
| **EU** | European Union |
| **GDPR** | General Data Protection Regulation |
| **GFF** | Gesellschaft für Freiheitsrechte |
| **IB** | Intelligence Bureau |
| **LDSG** | Landesdatenschutzgesetz |
| **LTTE** | Liberation Tigers of Tamil Eelam |
| **MAD** | Militärischer Abschirmdienst |
| **MLAT** | Mutual Legal Assistance Treaty |
| **MeitY** | Ministry of Electronics and Information Technology |
| **NIA** | National Investigation Agency |
| **NIRA** | National Identification and Registration Act |
| **NSA** | National Security Agency |
| **NTRO** | National Technical Research Organisation |
| **PAN** | Permanent Account Number |
| **PIL** | Public Interest Litigation |
| **PKGr** | Parlamentarisches Kontrollgremium |
| **RAW** | Research & Analysis Wing |
| **SAARC** | South Asian Association for Regional Cooperation |
| **SB** | Ständiger Bevollmächtigter |
| **SIGINT** | Signals Intelligence |
| **SNV** | Stiftung Neue Verantwortung |
| **SRDH** | State Residents Data Hub |
| **SSPAC** | Sigint Seniors Pacific |
| **TRAI** | Telecom Regulatory Authority of India |
| **UG** | Unabhängiges Gremium |
| **UIDAI** | Unique Identification Authority of India |

## Introduction

The year 2018 was significant for privacy and data protection in both India and Germany. While India introduced an exhaustive Draft Personal Data Protection Bill, Germany revised its existing data protection statute, the Bundesdatenschutzgesetz (BDSG) or the Federal Data Protection Law, to be streamlined with the new pan-European Union General Data Protection Regulation (GDPR).[1]

The way the two countries have dealt with the subject differs rather fundamentally. Germany was among the first countries in the world to have a data protection law, albeit at a regional level.[2] This was as early as 1970. India, on the other hand, began taking its first steps towards acknowledging data protection as an issue that might need exclusive regulation only in the 21st century. The Information Technology Act, 2000 contained a punitive provision for a business entity's negligence "in maintaining a reasonable security to protect ... data or information". By 2011, a set of "Rules" governing handling of data by businesses were introduced under the Act by executive action. It was as late as 2017 that the country recognised privacy as a fundamental right. Meanwhile in Germany, the Grundgesetz or Basic Law that came into being in West Germany soon after the War, codified the right to "privacy of correspondence, posts and telecommunications". It extended to all of Germany after reunification. In addition to this, German lawmakers and jurists developed further positions over time on issues such as the right to informational self-determination. With the revised BDSG-Neu today, it has taken yet another step forward in further developing its legal framework on the matter.

The countries' respective experiences of privacy abuses through the years also offer a stark contrast that has incontestably impacted their philosophies and policies on privacy and data protection today. Germany, as a whole, saw two waves of institutionalised privacy violations. One, with the large-scale profiling that took place under the Nazi regime in the pre-Second World War years. Second, with Soviet surveillance in East Germany after the war and before reunification. India, by comparison, had seen scattered, individual cases of privacy violations in the 20th century. The possibility of mass-scale privacy violation only entered the popular consciousness at the turn of the millennium.[3] This too, was largely as a function of the proliferation of businesses built on digital technologies. India offered a fertile ground for such businesses, particularly those from the USA. As the second most popu-

[1] The resulting reformed law is referred to as the BDSG-Neu.

[2] The state of Hessen passed a local data protection law in 1970. Called the Hessisches Datenschutzgesetz (HDSG), or Hessian Data Protection Act, it is credited with being the first data protection regulation in the world.

[3] Although the possibility of mass-scale privacy violation became more widely acknowledged in the Indian context with the proliferation of digital technologies, the idea of state-enabled violation of privacy did come up in the Constituent Assembly debates of the 1940s. We explore that further later in the paper.

lous country in the world after China, coupled with its openness to foreign investments, India became an attractive and lucrative proposition for these businesses, by virtue of the sheer volume it promised. However, given the country's colonial past, "data colonisation" was a fear that began to be articulated soon after, often with varying motivations—either when fighting against an exploitative practice like Facebook's anti-net neutrality Free Basics programme or when building support for protectionist policies such as a proposal to introduce strict data localisation measures.

Why, then, with such diametrical differences, must India and Germany be compared? These points of strong contrasts are exactly what make the exercise illuminating on how events, attitudes, and geopolitical realities have impacted the current privacy and data protection policies in the two countries. For the Indian context, studying the German example offers insights into the issues that may emerge as future sites of contestation. One such example is the census. For a large, diverse, and populous country such as India, census data has been central in designing central government's policies and welfare programmes. There has so far been no large-scale public disaffection in India against the exercise or the manner in which it is carried out, unlike in 1980s Germany, which saw citizens boycotting the exercise and the Constitutional Court stepping in. The movement led to Germany recognising the right to informational self-determination. In India, diffused murmurs of disapproval over potential privacy violations through the census exercise are beginning to be heard now. Government officials now claim willingness to incorporate principles of data protection in the census as it prepares to go digital with the mammoth nationwide exercise.[4]

While there is much that sets these two countries apart, their political and economic status in their respective regions gives them common ground. Germany was one of the six founding members of the European Union. India was one of the founding countries of the (relatively smaller) grouping of the South Asian Association for Regional Cooperation, or SAARC. According to the International Monetary Fund's World Economic Outlook for October 2019, Germany had the highest GDP in the European Union.[5] Within the SAARC countries, India had the same position according to the same IMF data.[6] Both countries carry significant political capital in their respective regional groupings. Comparing these two, then, also provides a barometer of sorts of how the European Union and the SAARC would compare.

---

[4]Sreevatsan, Ajai, "'We Have to Factor in Data Privacy in Census Design and Methodology'", *Mint*, 22 January 2018, https://www.livemint.com/Politics/04X1G5qiklWynGdtIxyAuO/We-have-to-factor-in-data-privacy-in-census-design-and-meth.html.

[5] "GDP, current prices, European Union", IMF, accessed 14 November 2019, https://www.imf.org/external/datamapper/NGDPD@WEO/OEMDC/EU?year=2019.

[6] "GDP, current prices, manually selected country group: Afghanistan, Bangladesh, Bhutan, India, the Maldives, Nepal, Pakistan and Sri Lanka", IMF, accessed 14 November 2019, https://www.imf.org/external/datamapper/NGDPD@WEO/AFG/BTN/IND/NPL/PAK/MDV/BGD/LKA?year=2019.

Another point where a comparison appears practical is that of legislation. When India released its Draft Personal Data Protection Bill in July 2018, it had hardly been two months since the enforcement of the GDPR in the EU. This led to various comparisons of the Bill with the EU Regulation, from where it appears to borrow a fair amount of phrasing and structure. A comparison with a particular EU jurisdiction where the GDPR has been applied certainly provides clearer and more practical points of juxtaposition. In this, Germany stands out for its decades of experience in enforcing and updating statutes on data protection, privacy, and related spheres.

The current point in time points to the urgency of undertaking a comparative study of this sort. The last decade has inarguably seen some of the most defining shifts in the debates and policies surrounding data protection and privacy across the world. These shifts were spurred on by events and movements, the ripples of which extended far beyond national borders. The most path-breaking of these was, without question, the Snowden revelations of 2013. The US National Security Agency contractor Edward Snowden blew the whistle on the country's sweeping global spying programmes, exposing how regular individuals and heads of states alike were compromised. Diplomatic standoffs ensued, as did large-scale public awareness of the various ways in which it was possible to trace, profile, and surveil a person. While this happened, a young Austrian activist, Max Schrems, was taking a global social media conglomerate to court in Ireland, putting the wheels in motion for changes in transatlantic commercial data transfers. His legal battle with Facebook, which started in 2011, set pan-EU precedents when it comes to transfers of data outside of Europe and has been significant in setting standards for acceptable forms of data processing for the EU. In yet other developments, in 2014 the European Court of Justice recognised the Right to Be Forgotten. And all this while, deliberations were on for a new pan-EU regulation to govern data protection with the General Data Protection Regulation (GDPR). By the time this regulation came into force, a global data protection scandal had revealed how democracies could be manipulated—consultancy firm Cambridge Analytica had exploited Facebook's terms of service to profile, target, and manipulate US voters in the 2016 presidential elections and UK voters in the EU referendum the same year. The impacts of and the reactions to these events have been a reflection of nothing less than the strength and integrity of democracy, democratic processes, and democratic institutions in the countries involved.

This research report analyses the issues of privacy and data protection as they have arisen in India and Germany, and the way that they interact with the ideas of individual rights and government accountability. It compares the two countries' approaches to privacy and data protection on four counts: the key historical events and factors; state surveillance; functioning and deployment of biometric government IDs; and the legal frameworks (in India's case, the *proposed* legal framework) governing data protection and protecting an individu-

al's right to privacy. In examining these four aspects, this comparative study explores, among other things, the right to privacy granted to and/or wrested by the individual within a state machinery and how that affects the relationship imagined between the citizen and the state. With this, it also explores the ideas of accountability and transparency in the two countries within the rubric of data protection and privacy.

The first section delves into the historical evolution of the approach to privacy as a right in Germany and India, followed by the countries' moves in data protection regulation. The chronological point of departure for both is after the Second World War, when Germany saw the toppling of the Nazi regime in 1945 and India the official departure of the British colonial government in 1947. It goes on to analyse how and why certain constitutional protections were introduced (informational self-determination for Germany) or rejected (privacy as a fundamental right, in the initial years, for India). It uses these threads to connect with current motivations animating data protection policies in the two countries.

The second section focuses on the architecture and functioning of state surveillance and the oversight mechanisms that assign accountability to law enforcement and government institutions. It focuses on India's lack of judicial and parliamentary oversight over intelligence agencies, alongside Germany's recently revised oversight regime. The section also examines the impact of and the reaction to the Snowden revelations of 2013 to illustrate the extents of government accountability that the two democracies had room for.

The third section is centred on the biometric identity tools in Germany and the biometric identity programme in India. It takes into consideration the deployment of biometric passports in Germany after 2005 requirements prescribed by the European Union, as well as the use of biometrics in the national ID instrument called the Personalausweis. In India, the biometric-linked unique identity programme Aadhaar serves as a point of comparison. The two are analysed for the extent of function creep and the resulting impact on individuals' control over their personal data.

The last section analyses the legal regimes in both countries, taking as points of comparison the GDPR and the BDSG-Neu in the German context and the Draft Personal Data Protection Bill, 2018, authored by the B N Srikrishna Committee, in the Indian context. It begins with a comparative analysis of the legal rights conferred upon individuals. This is followed by an analysis of data transfer obligations and how they impact these individual rights. Finally, it explores the kinds of exemptions afforded to governments and government agencies under the two regimes, and how these fare when it comes to accountability and transparency.

# 1. Data protection and privacy through the years: A look at the historical evolution of regulation in India and Germany

This section describes how India and Germany have approached data protection legally and politically. There have been significant parallel developments in recent years. In India, a draft bill on privacy prepared by a committee led by former Supreme Court judge Justice B N Srikrishna was released to the public in July 2018. Shortly before, in May 2018, Germany with the rest of the European Union had come under the purview of the General Data Protection Regulation (GDPR). A comparison of past events leading up to this point provide a better insight into the motivations, apprehensions, and the concerns of the two countries.

The end of the Second World War in 1945 serves as an important time-marker to start this comparison, as it establishes a significant point in the very nationhood of both the countries. Germany began its journey as two nations under military occupation, while in India, the end of the war precipitated the departure of the British imperial government two years later and the establishment of an independent sovereign nation of India. Political events in the years that followed set very different priorities for both the countries. These set the tone for political and legislative action for the years ahead.

## 1.1. Evolution of the Indian position

The Indian Constituent Assembly debates from the 1940s show how lawmakers of independent India considered and then discarded the idea of instituting privacy as a fundamental right—something that would come back under legal consideration seven decades later, and finally be granted the status in August 2017.

Legal scholar Chinmayi Arun identifies two kinds of "privacies" that were considered in these debates: one that dealt with secrecy of correspondence and another that offered protection against unreasonable search and seizure.[7] The debates show that a primary concern while deliberating the fundamental right to privacy and/or secrecy of communication was the impediments it could create for the administrative class to carry out state functions. Those who opposed the introduction of the right saw an architecture of permits, sanctions, and approvals as something that would slow down the work of a bureaucracy dealing with a population as large as India's.[8]

[7] Arun, Chinmayi, "Paper-Thin Safeguards and Mass Surveillance in India", *National Law School of India Review*, no. 26 (2014): 106-108.
[8] The 1951 Census of India recorded the country's population at 361,088,090 persons.

The Draft Report of the Indian Sub-Committee on Fundamental Rights presented in April 1947 contained an Article 9(d), which guaranteed the right to secrecy of correspondence and the right against unreasonable search and seizure. Interestingly, here, India was already looking to pre-war Germany. This section was adapted from the Weimar Constitution,[9] where Article 117 guaranteed secrecy of postal, telegraphic, and telephonic communication, while Article 115 said that the dwelling of every German was inviolable.[10] Opposition to the inclusion of the right came from Constituent Assembly members such as Alladi Krishnaswamy Iyer, who said, "A clause like this may checkmate the prosecution in establishing any case of conspiracy or abetment in a criminal case and might defeat every action for civil conspiracy, the plaintiff being helpless to prove the same by placing before the court the correspondence that passed between the parties, which in all these cases would furnish the most material evidence ... On a very careful consideration of the whole subject, I feel that inclusion of such a clause in the chapter on fundamental rights will lead to endless complications and difficulties in the administration of justice." Fellow member BN Rau too felt it would impede criminal investigations and said, "Often, in the course of investigation, a police officer gets information that stolen property has been secreted in a certain place. If he searches it at once, as he can at present, there is a chance of his recovering it; but if he has to apply for a court's warrant, giving full details, the delay involved, under Indian conditions of distance and lack of transport in the interior, may be fatal."[11] Here, it is pertinent to mention for the record those in the Constituent Assembly who argued on the other side of this issue. Those like Kazi Syed Karimuddin, Pandit Thakur Das Bhargava, Somnath Lahiri, and indeed, father of the Indian constitution Dr B R Ambedkar himself, had argued in *favour* of different facets of a right to privacy. These included right of the people to be secure in their houses against unreasonable search and seizure and also a right to privacy in correspondence.[12]

When discussing privacy in 2017, case law became an important factor in formulating a position. By then, various cases had covered this ground from the vantage points as diverse as health and medical information, state surveillance, confidentiality of financial details, intrusive media reportage, and even sexual violence.[13] For example, a 1998 Supreme Court case, titled Mr X vs Hospital Z, concerned a hospital that had divulged the petitioner's HIV

[9] Matthan, Rahul, *Privacy 3.0*, 2018th ed. (HarperCollins Publishers India): 80.
[10] "The Constitution of the German Reich, Translation of Document 2050-PS, Office of U.S. Chief of Counsel", Ithaca, New York: Cornell University Law Library. Accessed 26 April 2019. http://reader.library.cornell.edu/docviewer/digital?id=nur:01840#page/7/mode/1up
[11] Matthan, *Privacy 3.0*, 83-84.
[12] Arun, "Paper-Thin Safeguards and Mass Surveillance in India": 105-108.
[13] Centre for Communication Governance, National Law University, Delhi detailed 37 cases connected to the Right to Privacy in India between 1964 and 2015. "The Indian Supreme Court on the Right to Privacy: 63 Years of Progress", *The CCG Blog*, 13 August 2017, https://ccgnludelhi.wordpress.com/2017/08/13/h/.

positive status to his fiancée. This led to the petitioner's wedding being called off and subsequent social ostracisation. The petitioner sued the hospital for not maintaining confidentiality. The court here adjudged that while the right to privacy was "an essential component of (the) right to life", the fiancée in this case had a right to know, as it would have posed a health risk to her. The hospital, the court ruled, violated neither privacy nor the rules of confidentiality in this case.

Among the most cited in Indian case law is Kharak Singh vs the State of UP and Others from 1962.[14] The case concerned a person who had been charged with dacoity but then later let off for lack of evidence. However, he continued to be on the receiving end of domiciliary visits by police personnel at nights. A majority of the six-judge bench of the Supreme Court ruled that in this case, although privacy was not a constitutional right, the repeated domiciliary visits by the police at night did constitute a violation of fundamental rights. In a minority judgement, the sole dissenting judge, Justice Subba Rao, read the right to privacy as an essential component of Article 21 of the Indian Constitution, which guarantees the right to life and liberty. In a dramatic departure in 2017, when the Supreme Court adjudged the right to privacy to indeed be a fundamental right, the majority judgment in the Kharak Singh case was overruled.

As concerns data protection, there was an attempt to introduce the same in 2011. This was not done by the passage of a separate Act, but with the introduction of a new set of "Rules" under Section 43A of the Information Technology Act, 2000. Section 43 A deals with the "compensation for failure to protect data" when the failure is on the hands of a "body corporate" or a private firm or company engaged in business. Under this Act, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, or IT Rules 2011, were introduced. The Rules prescribed conduct for private organisations and businesses when it came to processing, collection, storage, and other kinds of data handling. These were, however, criticised for falling "short of internationally accepted data protection standards"[15] and were described as "not a model of clarity".[16] For one, the Rules weren't exhaustive—the short title and commencement, definitions, and the rules themselves were contained in just five pages. Second, it did not apply to public bodies or the government. Furthermore, while the definitions under the Rules de-

[14] Kharak Singh vs the State of UP and Others, Supreme Court of India, 1962.

[15] Acharya, Bhairav, "Comments on the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011", Centre for Internet and Society, 31 March 2013. https://cis-india.org/internet-governance/blog/comments-on-the-it-reasonable-security-practices-and-procedures-and-sensitive-personal-data-or-information-rules-2011.

[16] Saikia, Nandita, "On The Indian Government's Clarification On IT Rules And Personal Data", *MediaNama* (blog), 26 August 2011, https://www.medianama.com/2011/08/223-on-the-indian-governments-clarification-on-it-rules-and-personal-data/.

fined both personal information and sensitive personal data, the protections offered and the fines prescribed were solely for sensitive personal data. This class of data included passwords, financial information, health conditions, sexual orientation, medical records and history, biometric information, and any details related to these. This left out communications data, profiling information, identifying information such as names, addresses, and the like, among others. The Rules mandated that "body corporates" disseminate a privacy policy; that they obtain written consent from the data subject who is described throughout as the "provider of sensitive personal data or information"; and that the data subject be told about the collection of information, purpose, and recipients of the same. The Rules allowed data to be transferred to another body corporate within India when necessary for performance of contract or under consent from the "provider of information".

The terminology in these Rules—such as "provider of information"—left much open to interpretation. As far as the operations of the "body corporates" were concerned, the government had to issue a clarification to the effect that it applied only to those operating within India,[17] thereby leaving the coast clear for foreign business process outsourcing companies. Puzzlingly, this clarification came not in the form of a further amendment or another executive order but a press release from the Ministry of Communications and Information Technology (MeitY).

Legal consultancy Linklaters found no "example of enforcement action taken under the IT Rules, 2011"—a testament to their lack of efficacy. In fact, in its report, the BN Srikrishna Committee itself commented on the Rules' "unduly narrow" definition of personal data and its "problems of implementation due to delays in appointments to the adjudicatory mechanisms". The Committee also pointed to its lack of jurisdiction over public bodies, saying, "Ensuring that the state respects the right to privacy of the citizen should be a key aim of any data protection framework building on the fundamental right to privacy." However, in the very next line, it qualifies this requirement, saying, "it must be recognised that several purposes for state processing of personal data may relate to the public interest", and that "specific purpose-based exemptions" for "national security, investigating crime, protecting revenue etc." must be created within the law.[18] This is in line with the Justice B N Srikrishna Committee's own formulation in the Draft Personal Data Protection Bill, where state, legislature, and security agencies are given a wide range of exceptions when it comes to data processing.

[17] "Clarification on Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 Under Section 43A of the Information Technology ACT, 2000", Ministry of Communications & Information Technology, 24 August 2011. https://pib.gov.in/newsite/erelease.aspx.

[18] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, "A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians", 27 July 2018: 6-7.

In addition to these efforts towards data protection in India, there were other formal discussions and consultations at the administrative and political levels earlier, but to no conclusion or state action. In 2012, for example, the central government had constituted a "Group of Experts" headed by the former chief justice of the Delhi High Court, Justice A P Shah. This group released a report defining the principles governing the right to privacy. This was to facilitate the "authoring of the Privacy Bill" for the government[19]—something that took another five years to even get started. Before the central government got started on this project, five private member Bills[20] on privacy were floated until 2016, though none came up for discussion in Parliament.[21] The current Bill, however, was drafted by a committee formed directly under the central government's Ministry of Electronics and Information Technology (MeitY) in July 2017. At the head of the government committee this time was again a jurist: former Supreme Court judge Justice B N Srikrishna. Also, the Committee was more specifically tasked with developing a framework for data protection. The committee submitted its Bill in July 2018 along with a report on its work.

At an institutional level, the debate on privacy had begun to shift when the Supreme Court started hearing a collection of Public Interest Litigations (PILs) in 2012 challenging the constitutional validity of the nationwide biometric-linked identity programme, Aadhaar. This process began in 2012, and a decision in the matter was finally reached in 2018. The events mentioned in the paragraph above took place alongside the hearings in the matter. Along the way, in 2017, an important legal milestone was crossed with privacy being adjudged a fundamental right. Briefly, the events were as follows. With the 2012 Public Interest Litigation, the petitioners in the Aadhaar case argued that the programme, in its collection, handling, and linking of citizens' biometric data, violated the right to privacy. Responding to this, government counsel, Attorney General Mukul Rohatgi, argued that the right to privacy does not exist.[22] He referred to previous cases, like the Kharak Singh case from the 1960s, when majority bench did not recognise such a right, to make this argument.[23] The government's assertion that privacy was not a fundamental right put another set of legal events into motion. The Supreme Court in August 2015 referred the matter of identifying privacy

[19] "Group of Experts on Privacy Submit Report" (Press Information Bureau, Government of India, October 18, 2012), https://pib.gov.in/newsite/PrintRelease.aspx?relid=88503.
[20] Private Member Bills are bills formulated and floated by the members of Parliament instead of government committees.
[21] Dutta, Prabhash K, "Right to Privacy: 5 Bills yet No Law, How Parliament Has Dealt with Personal Data Protection", *India Today*, 24 August 2017, https://www.indiatoday.in/india/story/right-to-privacy-fundamental-right-parliament-1031136-2017-08-24.
[22] Choudhary, Amit Anand, "No Fundamental Right to Privacy to Citizens: Centre Tells SC", *The Times of India*, 22 July 2015, https://timesofindia.indiatimes.com/india/No-fundamental-right-to-privacy-to-citizens-Centre-tells-SC/articleshow/48171323.cms.
[23] The part of this judgment which did not recognise privacy as a right was later overruled by the nine-judge bench that delivered the 2017 privacy verdict.

as a fundamental right to another nine-judge bench of the Supreme Court. Two years of arguments later, in 2017, the bench finally decreed it to be a fundamental right.[24] The nine judges unanimously recognised it as an intrinsic part of the right to liberty and the right to life under Article 21 of the Indian Constitution. This 2017 decision of the Supreme Court in turn impacted the course of the parallel Aadhaar hearings. With the Aadhaar judgment of 2018 that followed, several provisions of the erstwhile Aadhaar Act[25] were deleted, although the programme on the whole was not found to be violative of privacy. The Draft Data Protection Bill of 2018, released by the B N Srikrishna Committee a couple of months before the 2018 Aadhaar judgment, served as the next definitive step on the Indian route to a comprehensive legislation in the field.

We see two concerns at play in the 2017 and the 2018 judgments of the Supreme Court of India. One is that of protecting state interest and state authority, and the other is that of regulating businesses, particularly by foreign players.

The 2017 decision of the Supreme Court focused on the value of privacy as a constitutional right, of which informational privacy and data protection was but a part. "Informational privacy is a facet of the right to privacy", says the judgment. It then goes on to enumerate "privacy concerns against the state" and the ways in which state-sponsored surveillance and profiling of citizens can harm the exercise of fundamental rights. Justice SK Kaul even recommends looking to the EU GDPR as a guiding point in the judgment, saying, "... formulation of data protection is a complex exercise which needs to be undertaken by the State after a careful balancing of privacy concerns and legitimate State interests, including public benefit arising from scientific and historical research based on data collected and processed. The European Union Regulation of 201629 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data may provide useful guidance in this regard."

The text of the judgment dwells at length on the matter of "proportionality"—defining the legitimate and proportionate extent of state intrusion into privacy. Among the many examples it took from European case law to illustrate this was the Uzun vs Germany case from the European Court of Human Rights, delivered in 2010.[26] Here, the state investigative agency—North Rhine-Westphalia Department for the Protection of the Constitution (Verfassungsschutz)—carried out surveillance on a person with links to the Anti-Imperialist Cell, who was convicted for planting bombs outside the houses of members of parliament,

[24] Justice K Puttaswamy (Retd) and Another v Union of India (Supreme Court of India 24 August 2017).
[25] The Aadhaar (Targeted Delivery of Financial & Other Subsidies, Benefits & Services) Act, 2016.
[26] Uzun vs. Germany (The European Court of Human Rights (Fifth Section) 2 December 2010).

former members of parliament, and also the Peruvian Honorary Consulate. To establish the case, the agency collected GPS car data on the applicant in the case and his accomplice. The extent of surveillance and the consequent admissibility of the evidence here was what was contested. The European Court of Human Rights held the surveillance to be proportionate here, saying, "There are a number of elements relevant to a consideration of whether a person's private life is concerned by measures effected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor."[27] The Indian Supreme Court found that in the case, "a fair balance is struck between the general interest of the community and the interests of the individual".[28]

As far as regulating commercial activity with personal data is concerned, the text of the Draft Bill appears to keep that concern front and centre.[29] This is evident from its accompanying report, which is titled: "A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians". After it prominently mentions the "transformative potential" of the digital economy to improve lives in India, and also enumerates the harms from both the state and private players in misuse of personal data, the Committee goes on to say in the opening chapter of the report: "It is our view that any regime that is serious about safeguarding personal data of the individual must aspire to the common public good of both a free and fair digital economy."[30]

Both these concerns—that of state interest and that of creating a favourable business environment—place the state and commerce as active determinants of an individual's realisation of her right to privacy. Processing of data by public bodies and security agencies is repeatedly formulated as legitimate and necessary. As for businesses, data is repeatedly posited as a value-holding asset waiting to be mined rather than an entity with a personal dimension inherently deserving of protection.

By the time the deliberations of the Supreme Court and the government-appointed committee had ended, various privacy violations through unsecure sharing of Aadhaar details had been recorded, the global Cambridge Analytica scandal had already impacted over 250,000 Indian Facebook users (by the tech giant's own admission), and both homegrown digital wallet Paytm and global player in the sector Google Pay had been accused of sharing user data with third parties without consent. As of the autumn of 2019, this Draft Bill is yet to be

[27] Uzun vs. Germany (The European Court of Human Rights (Fifth Section) 2 December 2010).
[28] Justice K Puttaswamy (Retd) and Anr v Union of India (Supreme Court of India 24 August 2017).
[29] Gupta, Apar, and Uppaluri, Ujwala, "A Fundamental Error", *The Hindu*, 1 August 2018, sec. Opinion. https://www.thehindu.com/opinion/lead/a-fundamental-error/article24566374.ece.
[30] B N Srikrishna Committee, 7.

tabled in the Indian Parliament. India is yet to join the 118 countries of the world that have enacted a comprehensive data protection law.[31] Further delays are sure to impact the rights of Indian data subjects going forward.

### 1.2. The German journey

Germany is seen as a global pioneer in data protection for various reasons. It was the first country in Europe to have passed a data protection act at the state level in the state of Hessen in 1970 and at the federal level in 1978 as the Bundesdatenschutzgesetz or BDSG.

Once the GDPR was finalised in 2016, Germany was among the first countries in Europe to revise its local data protection law, the BDSG. An updated and reformed BDSG-Neu was introduced as early as July 2017—a year ahead of the 25 May 2018 deadline for the GDPR.

As evidenced by the deliberations of the Constituent Assembly, the Supreme Court and the B N Srikrishna Committee, India has repeatedly looked towards Europe in general and Germany in particular in developing its position on privacy and data protection. In this, understanding the events, concerns, and preoccupations that animated the German position and its evolution is pertinent.

The dominant view on the matter holds that large-scale data collection on and surveillance of citizens in Nazi-era Germany, and later in the Soviet-era East Germany, left the country with heavy caution against large-scale exercises involving personal data collection, regardless of the entity collecting the data. Unlike in India, state activities are not considered legitimate by default. This reading has been extended not just to recent developments like the GDPR but also to older events, like the population census decision in the 1980s.

In his seminal work of 2001, Edwin Black details how (in the absence of modern-day computers), the Third Reich tabulated, processed, and acted on extensive data collected on the German population. This, says Black, was largely aided and expedited by the mechanisation offered by technology company International Business Machines or IBM (then Dehomag in Germany) and its Hollerith machines.[32] These machines, initially installed in the census complex in Berlin's Alexanderplatz, sorted through population data on "punch cards". These cards recorded data across rows and columns indicating certain characteristics such as religion, language, profession, and others with holes at corresponding spots in the resulting table. These cards were then sorted through the Hollerith machines to arrive quickly at sections of the population the Nazi government wanted to expel or exterminate.[33]

---

[31] Banisar, David, "National Comprehensive Data Protection/Privacy Laws and Bills 2019", ARTICLE 19: Global Campaign for Free Expression, 1 August 2019. http://dx.doi.org/10.2139/ssrn.1951416.
[32] Black, Edwin, *IBM and the Holocaust: The Strategic Alliance Between Nazi Germany and America's Most Powerful Corporation*. Little, Brown & Company, 2001: 23-30.
[33] Ibid.

"There are historical explanations for the distrust and revulsion Germans feel toward state surveillance, which help explain the widespread belief that privacy merits special protection", says an analysis of data protection in Germany from the Bertelsmann Foundation.[34] "The Third Reich also systematically abused private data: It maintained a so-called index of Jews that listed the identity of all Jews dating back to their grandparents' generation. In addition, it relied on data collected during the Weimar Republic (1918–1933), including records of homosexuals. Nazi Germany's persecution of Jews and homosexuals proved that no matter the intent of the data-collecting entity, the collection of so much personal information about individuals could be dangerous in and of itself", it says.[35]

In a piece for The New York Times written in the wake of the Snowden revelations, Green Party member and Gesellschaft für Freiheitsrechte secretary general Malte Spitz also points to German history when speaking of the German attitude towards privacy infringements. "Although these two dictatorships, Nazi and Communist, are gone and we now live in a unified and stable democracy, we have not forgotten what happens when secret police or intelligence agencies disregard privacy. It is an integral part of our history and gives young and old alike a critical perspective on state surveillance systems", he writes.[36]

In the light of these excesses, post-war West Germany developed the "right to personality". It was called a Quellrecht, or "source right", since it was the source from which the development of the right to private life and that of the principle of informational self-determination flowed. The development of these happened through case law, with the legal principles linking the right to dignity, personality, and personal life being established early on. According to the legal scholars Paul M Schwartz and Karl-Nikolaus Peifer, German courts took these steps in the post-war period to develop the right to personality and "to solidify the notion of a right to privacy ground in the dignity of the individual".[37] Notably, in the early 1900s, this very right was rejected by legal commentators in Germany for being too broad and amorphous. That, however, changed after the Second World War, which made the framers of the Basic Law see the protection of personality rights for dignity as significant.[38]

---

[34] Freude, Alvar and Freude, Trixy, "Echoes of History: Understanding German Data Protection", Bertelsmann Foundation, 1 October 2016, https://www.bfna.org/research/echos-of-history-understanding-german-data-protection/.
[35] Ibid.
[36] Spitz, Malte, "Germans Loved Obama. Now We Don't Trust Him", *The New York Times*, 19 October 2018, sec. Opinion, https://www.nytimes.com/2013/06/30/opinion/sunday/germans-loved-obama-now-we-dont-trust-him.html.
[37] Schwartz, Paul M. and Peifer, Karl-Nikolaus, "Prosser's Privacy and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Concept", *California Law Review* 98, 2010: 1950.
[38] Schwartz and Peifer, "Prosser's Privacy", 1947-8.

The German Basic Law does not recognise a right to privacy or to data protection in as many words. "We still don't have the parliamentary right to data protection in Germany. We also don't have a fundamental right to privacy. What we have is Article 1 on Human Dignity and we have Article 2 on the right to act like whoever you want or Allgemeine Handlungsfreiheit. These two are combined in the German courts' verdicts, and they developed from these two fundamental rights the right to private life", says Malte Engeler, judge at the Administrative Court of Schleswig-Holstein, former deputy head of the supervisory unit of the data protection authority of Schleswig-Holstein, and representative of the German data protection authorities in the Article 29 Working Party subgroups.[39]

Turning to case law, we can see the key turning points in this process of drawing out other rights from the "source right" of the right to personality. In this, the 1954 Schacht Letter Decision of the Bundesgerichtshof is significant. It was with this case that the Federal Supreme Court read the right of personality into the Civil Code. This was further solidified in the 1958 Gentleman Rider case, in which the court prescribed damages for the violation of the right of personality as well.[40] As part of personality rights, case law also established the right to a second chance in society. This was with the Lebach case in 1973. Here, a murder convict approached the court against extensive media coverage of him completing his prison term and nearing release, arguing it would hamper his chances of reintegrating into the mainstream. The German Federal Constitutional Court, or Bundesverfassungsgericht, ruled in his favour, recognising his right to a second chance in society.

More recently, in the Federal Constitutional Court decision on online searches in 2008, the Karlsruhe court ruled that a 2006 amendment of the Act on the Protection of the Constitution in North Rhine-Westphalia, allowing the use of malware such as trojans for online searches, was unconstitutional.[41] In their analysis of the case, legal scholars Gerrit Hornung and Christoph Schnabel say that the court found the rights covering secrecy of telecommunications and sanctity of home to be inadequate when applied to online searches of computers and IT systems. The Federal Constitutional Court then read into what it called the "gap-closing function of the general personality right" to develop a right that covers "IT systems that may—as such, or within a network—store personal data to an extent that the searching of the system could disclose important parts of the conduct or life of a person or even a significant image of his/her personality".[42]

---

[39] Engeler, Malte, personal interview, 12 February 2019.

[40] Schwartz and Peifer, "Prosser's Privacy", 1951.

[41] BVerfG, Judgment of the First Senate of 27 February 2008 - 1 BvR 370/07 -, paras. (1-333), http://www.bverfg.de/e/rs20080227_1bvr037007en.html.

[42] Hornung, Gerrit and Schnabel, Christoph, "Data Protection in Germany II: Recent Decisions on Online-Searching of Computers, Automatic Number Plate Recognition and Data Retention", *Computer Law & Security Review* 25, no. 2 (January 2009): 116, https://doi.org/10.1016/j.clsr.2009.02.008.

The Federal Constitutional Court's decision in the Census Case of 1983, known as the Volkszählungsurteil, marked a watershed moment in the development of a data protection regime in Germany. Hornung and Schnabel hold it to be the "very key to the German view on data protection".[43] With this decision, the Federal Constitutional Court created a constitutional right to informational self-determination. This landmark development was the result of an equally significant civil movement against mass data collection of citizens in the 1980s. In these anti-census protests in West Germany, protestors questioned the need for the number and kind of questions posed in the census. Some protesters resorted to not answering the questions at all, while others to "accidentally" damaging the forms or writing illegibly.[44] In its 1983 decision, the court placed constitutional protection over personal data in Germany and recognised individual control over the amount and extent of use of their personal data. It prohibited the creation of citizen profiles with unique identifiers, and even the sharing of data between government departments after a one-time collection. The decision led to the amendment of the BDSG in 1990, where the court's decisions and observations were taken into account in the form of building in consent requirements, transparency, and prevention of abuse by government agencies. Hornung and Schnabel see the development of this right as distinct from and complementary to the right to privacy. They find it strengthens participation in the democratic process. "If citizens cannot oversee and control which or even what kind of information about them is openly accessible in their social environment, and if they cannot even appraise the knowledge of possible communication partners, they may be inhibited in making use of their freedom. If citizens are unsure whether dissenting behaviour is noticed and information is being permanently stored, used and passed on, they will try to avoid dissenting behaviour so as not to attract attention", in effect making freedom of speech and choice "virtually impossible".[45]

Matthew G Hannah traces the root causes of public discontent against the census exercise in the 1980s to various factors, the catalysing one being the 1970s government crackdown on the Red Army Faction, where the law enforcement depended on extensive data collection to trace and track the members of the body and its meetings and activities.[46] Hornung and Schnabel say public opinion in the German Census Case was characterised by a "general resentment against growing surveillance and data processing".[47]

---

[43] Hornung, Gerrit and Schnabel, Christoph, "Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination", *Computer Law & Security Review* 25, no. 1 (January 2009): 85, https://doi.org/10.1016/j.clsr.2008.11.002.

[44] Hannah, Matthew G., *Dark Territory in the Information Age: Learning from the West German Census Controversies of the 1980s* (Burlington, Vt: Ashgate, 2010): 56.

[45] Hornung and Schnabel, "Data Protection in Germany I", 85-86.

[46] Hannah, *Dark Territory*: 6-23.

[47] Hornung and Schnabel, "Data Protection in Germany I", 85.

This resentment against extensive data processing could be seen even decades after the anti-census mobilisation. For example, in 2007, when CDU politician and then Secretary of Interior Wolfgang Schäuble proposed laws regarding online data retention and surveillance of computer systems, activists resisting the move referenced Soviet-era surveillance. They termed him "Stasi 2.0", complete with posters and memes for online circulation. The reference, of course, was to the East German State Security Service called Staatssicherheit, or Stasi for short. The Stasi had indulged in extensive and oppressive means of surveillance and suppression of dissenting voices. Similar terminology was employed for former US President Barack Obama in the wake of the Snowden revelations of 2013. Malte Spitz reacted to the US collection of mass data under the NSA's PRISM programme drawing on the history of the Stasi in East Germany. "In Germany, whenever the government begins to infringe on individual freedom, society stands up. Given our history, we Germans are not willing to trade in our liberty for potentially better security. Germans have experienced firsthand what happens when the government knows too much about someone. In the past 80 years, Germans have felt the betrayal of neighbors who informed for the Gestapo and the fear that best friends might be potential informants for the Stasi", he wrote in a June 2013 column for the New York Times.[48]

Apart from apprehensions regarding government collection of data, there was also a preoccupation with cashing in on the economic opportunities that effective participation in the digital society had to offer. The internet policy scholars Julia Pohle et al see the beginning institutionalisation of the "information society" discourse in Germany and describe government action at the time as a catching up of sorts to global circumstances and movements. "Like most other countries, Germany began to develop a political response to the internet and its societal impact in the early 1990s, when the discussion on the information society started to unfold on both the national and international level. The concept of 'information society' was commonly used as a metaphor to capture the importance of information for economic and societal progress", they say.[49]

It was with this historical arc that we finally saw Germany welcoming the General Data Protection Regulation (GDPR) in 2018, being one of the first countries to harmonise its local data protection law or the BDSG with the EU regulation. India, meanwhile, awaits the debate on and the passage of the Draft Personal Data Protection Bill, which features several provisions that are similar to the EU GDPR, including a provision for the right to be forgotten, the establishment of a Data Protection Authority, the principles of privacy by design, and the right to correction of data, among others. Later chapters will study these connections in detail.

---

[48] Spitz, "Germans Loved Obama".

[49] Pohle, Julia, Hösl, Maximilian, and Kniep, Ronja, "Analysing Internet Policy as a Field of Struggle", *Internet Policy Review* 5, no. 3 (25 July 2016): 7, https://policyreview.info/articles/analysis/analysing-internet-policy-field-struggle.

### 1.3. Identifying contrasts and drawing comparisons

One of the key differences in the way India and Germany have arrived at their current positions on privacy, and later on data protection, is the pace of evolution. Germany, as we saw above, started with an acknowledgement of the right to personality and the right to confidentiality of correspondence. It slowly built other derivative rights upon it through the decades as socio-political realities changed and technical capabilities developed. This evolution, which took decades in Germany, was condensed into a few years in India. A formal legal conversation exclusively on privacy could only begin when the government's unique biometric identity programme Aadhaar was challenged for violating privacy. The third section of the paper, which focuses on biometric IDs, shows how this legal challenge was the very thing that led to the recognition of the right to privacy. The conversation in this context did refer to other jurisdictions and decisions from different times in history. The response, however, was rooted in the country's 21st-century context, and its specific challenges of recognising and implementing a right to privacy while mass collection and processing of data took place.

More importantly, India did not have a collective, defining experience with large-scale, institutionalised surveillance like Germany did. As a result, one can observe in Germany, through the years after the war, a constant effort to keep individual lives inviolate. India, on the other hand, while transitioning from a colony to a sovereign state, focused on administrative ease when dealing with a large and diverse population when the question of privacy arose. These differences also inform the manner in which both the countries have developed their surveillance architectures and their ID systems. These themes are explored in the following sections.

## 2. State surveillance: A case for oversight

When comparing the intelligence regimes of India and Germany, the most striking difference to emerge is that of the accountability of the agencies. India currently lacks judicial and parliamentary accountability measures for its intelligence agencies. Attempts to introduce the same have been either too weak or have met with resistance. German intelligence agencies, on the other hand, have had strong parliamentary as well as judicial oversight for decades. These oversight mechanisms even saw a revision in 2016. However, these mechanisms and the recent amendments have received strong criticism locally on counts of superficiality, ineffectiveness, and for post-facto legalisation of problematic activities that were discovered only after harm was already done.[50] This section delves into the consequences of India's lack of an oversight mechanism and its securitisation[51] of the attempts at opening intelligence agencies to scrutiny. It also delves into how Germany failed to contain activities of the intelligence agencies outside the remit of the law despite having an oversight mechanism in place. A particular focus is on the collaboration with foreign investigative agencies as revealed by the documents leaked by whistleblower and former US National Security Agency contractor Edward Snowden.

To contextualise the above analysis, this section explores the structures and functioning of the key investigative agencies of Germany and India. In India, we see an endurance of colonial structures in a sovereign state. In Germany, we see gradual dismantling and rebuilding of structures that were in operation during and before the Second World War. Their origins and their subsequent evolution through the years illustrate the values toward which both the countries orient themselves when it comes to instituting democratic structures around the security apparatus.

### 2.1. Intelligence agencies in India

In 2018, nine investigation agencies and the office of the Commissioner of Police, Delhi, were officially authorised to intercept, monitor, and decrypt electronic communication and other digital data.[52] Among these, the agencies with the most far-reaching mandates are:

[50] Otwinowski, Martha, "Tailor-Made Laws: The State of Surveillance in Germany", *Index on Censorship*, 7 November 2016, https://www.indexoncensorship.org/2016/11/tailor-made-laws-the-state-of-surveillance-in-germany/.
[51] Wæver, Ole, "Securitisation and Desecuritisation", in *On Security*, ed. Ronnie D. Lipchutz, 1995, https://www.libraryofsocialscience.com/assets/pdf/Waever-Securitization.pdf.
[52] "The Gazette of India: Extraordinary, Order of the Ministry of Home Affairs (Cyber and Information Security Division)", 20 December 2018.

**Table 1**

| Agency | Area of responsibility and supervision |
|---|---|
| Intelligence Bureau (IB) | Domestic intelligence. Falls under the Union Ministry of Home Affairs. |
| Research and Analysis Wing (RAW or R&AW) | Foreign intelligence. Reports to the Prime Minister's Office. |
| Central Bureau of Investigation (CBI) | Corruption and special crimes. Under the superintendence of the Central Vigilance Commission or the Union Ministry of Personnel, Pension and Grievances (depending on the nature of the case under investigation). |
| National Investigation Agency (NIA) | Specially constituted after the 2008 Mumbai terror attack to look into cases of terrorism. It falls under the Union Ministry of Home Affairs. |

In a 72-year-old democracy, the Intelligence Bureau is a 132-year-old organisation. The body, about which little is known by the general populace or revealed by the government, falls under the administrative remit of the Union Ministry of Home Affairs. It was formed in 1887 by the erstwhile British Colonial government when the then British Home Secretary, Richard Asheton Cross, wrote to the then Viceroy in India, Frederick Hamilton-Temple-Blackwood, asking him to set up a system for "collection of secret and political intelligence in India". This was in the aftermath of movements against the British government and the struggle for Independence. Containing political dissent was key.

Blackwood wrote back months later with a plan on how he desired to "utilise in British India the services of the Police force and in Native States the existing means at the disposal of Political Officers, for the collection of intelligence on political, social and religious movements …"[53] Barring this British Colonial government letter exchange from 1887, there exists no other order—legal or otherwise—laying out the creation and mandate of the body. A retired IB official himself submitted a Public Interest Litigation in the Karnataka High Court in 2012, questioning the legal basis of the IB. The government here finally described the IB

[53] Rani, Sarita, "Snooping: The IB's Mandate Has Always Been to Protect India's Rulers from Indians", *The Wire*. Accessed 25 December 2018. https://thewire.in/government/snooping-the-ibs-mandate-has-always-been-to-protect-indias-rulers-from-indians.

as a "civilian organisation" without police powers.[54] Apart from this description by the government, there is no formal charter of duties for the IB. However, it appears from leaked reports and other events that it continues to function with an aim to contain dissent. In 2014, for example, an IB report on foreign-funded NGOs in India and their links to furthering "policy interests of western governments" was leaked to the media.[55] The following year, an Indian activist working for Amsterdam-headquartered NGO Greenpeace discovered that her movement out of India was curtailed thanks to an IB order.[56]

By contrast, more information is publicly available about the CBI. Unlike the IB, it has its own website, complete with FAQs for the layperson. It describes its mandate as that of investigating "serious crimes related to Defence of India, corruption in high places, serious fraud, cheating and embezzlement and social crime, particularly of hoarding, blackmarketing and profiteering in essential commodities". The origins of the body, like the IB, lie in pre-Independence India. It started as a government division in 1941 to investigate cases of bribery and corruption in "war related procurements". It was then called the Special Police Establishment. Five years later, this body was renamed the Delhi Special Police Establishment (DSPE) and placed under the DSPE Act of 1946. The two-page long text of the Act allows the central government, among other tasks, to constitute a police force, issue orders for its functioning, and appoint its officers. In 1963, the central government, via the union ministry of home affairs, constituted the Central Board of Investigation through an executive decision under the DSPE. The CBI has since investigated various high-profile corruption cases in India and has also been called on by the Supreme Court to take over investigations in certain other cases. But the CBI found itself in an existential dilemma in 2013. That year, hearing a public interest litigation challenging the constitutionality of the CBI, the Gauhati High Court quashed the 1963 resolution of the home ministry that was responsible for the formation of the agency. It found the government order lacking in procedural and legal technicalities (lack of oversight was not a consideration here).[57] The central government soon sought a stay on this decision from the Supreme Court. Since there hasn't been consequential further development on this case, the validity of the CBI under the DSPE Act continues to be a matter of dispute.[58]

---

[54] "Explain Intelligence Bureau's Legality, HC Tells Centre", *The Times of India*, 26 March 2012, https://timesofindia.indiatimes.com/india/Explain-Intelligence-Bureaus-legality-HC-tells-Centre/articleshow/12408605.cms.

[55] "Foreign-Funded NGOs Stalling Development: IB," *The Times of India*, 12 June 2014, https://timesofindia.indiatimes.com/india/Foreign-funded-NGOs-stalling-development-IB-report/articleshow/36411169.cms.

[56] "Priya Parameshwaran Pillai vs Union Of India And Ors", Delhi High Court, 12 March 2015.

[57] Navendra Kumar vs The Union Of India & Others, Gauhati High Court, 6 November 2013.

[58] Rao, YS, "The Mysterious Case of CBI's Legality", *Governance Now*, 3 June 2019, https://www.governancenow.com/news/regular-story/the-mysterious-case-of-cbis-legality.

As concerns the RAW, considerable secrecy and opacity surrounds the organisation. Even its formation in September 1968—widely attributed to India suffering losses in the Sino-Indian War of 1962 and the 1965 war with Pakistan—was kept under wraps until an article in the newsmagazine Illustrated Weekly wrote about it.[59] Although it is the chief foreign intelligence agency of one of the fastest growing democracies of the world, this organisation answers directly to the Prime Minister's Office without any external oversight by the parliament or the judiciary. There exists no public charter of its duties. It was formed by cleaving a foreign intelligence unit out of the IB following the two wars in the 1960s.[60] But the lack of accountability measures has left it open to the risks of being used to meet political ends of the parties in power. From 1975–77, when the then Indira Gandhi government imposed a nationwide state of emergency in the country, political dissidents were reported to have been put under RAW surveillance.[61] Former RAW officer B. Raman, however, has gone on record saying that the RAW was not involved in domestic political espionage at the time.[62]

The little that is known about the organisation and its activities today is from scholarly literature, journalistic reports, and memoirs and other writings of retired RAW officers. Ryan Shaffer, a scholar who has studied various aspects of the RAW's functioning in India's history, has pointed to the role the organisation has played in key geopolitical events in India's neighbourhood, like the formation of Bangladesh after separation from Pakistan in 1971 and the Liberation Tigers of Tamil Eelam (LTTE) uprising in Sri Lanka in the 1980s.[63] Yet efforts to bring the organisation under oversight have failed. Former officers such as B. Raman[64] and Retired Major General V. K. Singh[65] have argued for better accountability and more transparency in India's intelligence organisations, particularly the RAW. Raman drew attention to the lack of RAW's formal charter, legal backing, and even an acknowledgement of its existence in a newsmagazine column in 2010: "In the 1980s, when Indira Gandhi was the Prime Minister, a law was enacted by the Parliament banning strikes in the intelligence agencies. To my knowledge, that is the only Act of the Indian Parliament in which there is a reference to the R&AW by name. When that law was passed, nobody in the Parliament

[59] Shaffer, Ryan, "Unraveling India's Foreign Intelligence: The Origins and Evolution of the Research and Analysis Wing", *International Journal of Intelligence and CounterIntelligence* 28, no. 2 (3 April 2015): 260. https://doi.org/10.1080/08850607.2015.992754.
[60] Vaughn, Bruce, "The Use and Abuse of Intelligence Services in India", *Intelligence and National Security* 8, no. 1 (January 1993): 2–5. https://doi.org/10.1080/02684529308432188.
[61] Stanley A. Kochanek and Robert L. Hardgrave, *India: Government and Politics in a Developing Nation* (Boston: Thomson Wadsworth, 2000): 98.
[62] Raman, B. *The Kaoboys of R&AW: Down Memory Lane*, 2013 US edition (Lancer Publishers, 2007): 49–51.
[63] Shaffer, "Unraveling India's Foreign Intelligence", 259–268.
[64] "Making Intelligence Agencies Accountable," *Outlook Magazine*, 20 January 2010. https://www.outlookindia.com/website/story/making-intelligence-agencies-accountable/263866.
[65] Shaffer, "Unraveling India's Foreign Intelligence", 253.

thought it fit to ask: What is this R&AW about? When was it created? Who created it? Has its creation been approved by the Parliament?"[66]

Despite retired intelligence officers making a case for better accountability, the courts in India have not warmed up to the idea. In 2016, the Supreme Court quashed a public interest litigation asking for the RAW and the IB to be placed under a financial audit—a common practice in most western democracies. The court argued that such a mechanism will interfere with the secrecy these agencies require in order to maintain national security.[67]

Relatively more is known about the formation and composition of the National Investigation Agency (NIA), which was created in the aftermath of the terror attack in Mumbai in November 2008, which had the city under siege of Lashkar-e-Taiba terrorists for four days. The formation of the NIA was formally cleared the very next month after a late-night meeting of union cabinet ministers, followed by the introduction in the Parliament of a Bill to back the agency.[68] The NIA Act was passed in 2008 and the "central counter terrorism law enforcement agency in India" was born. The Act lays out procedural norms for the functioning of the NIA with respect to organisational structure and jurisdiction of cases.[69] The agency, according to the Act, can only take up investigation of cases at the direction of the central government. The Act is silent on accountability and oversight.

Besides these bodies, the Indian intelligence and surveillance ecosystem includes organisations like the National Technical Research Organisation (NTRO), which is responsible for "developing technology capabilities in aviation and remote sensing, data gathering and processing, cyber security, crypto systems, strategic hardware and software development, and strategic monitoring."[70] In addition, there is also the NATGRID or the National Intelligence Grid. Approved in 2011, the NATGRID serves as a consolidated searchable database for security and intelligence agencies. For communications interception, there exists the Central Monitoring System, or CMS—a centralised body for telephone and mobile phone interception, to which various intelligence bodies have access. Its formation was approved by the Cabinet Committee on Security, and it functions under what is known as the "Telecom En-

---

[66] Raman, "Making Intelligence Agencies Accountable".

[67] "Supreme Court Junks Plea Seeking To Make Intelligence Agencies Accountable", *NDTV.com*, 23 February 2016, https://www.ndtv.com/india-news/supreme-court-junks-plea-seeking-to-make-intelligence-agencies-accountable-1280316.

[68] "Finally, Govt Clears Central Terror Agency, Tougher Laws", *The Times of India*, 16 December 2008, https://timesofindia.indiatimes.com/india/Finally-govt-clears-central-terror-agency-tougher-laws/articleshow/3842368.cms.

[69] The National Investigation Agency Act, 2008, Accessed 27 September 2019. https://mha.gov.in/sites/default/files/The%20National%20Investigation%20Agency%20Act%2C%202008_1.pdf.

[70] "National Tech Research Body to Be Housed in Hyderabad", *The Hindu Business Line*, 25 February 2010, https://www.thehindubusinessline.com/todays-paper/tp-economy/National-tech-research-body-to-be-housed-in-Hyderabad/article20163734.ece.

forcement Resource and Monitoring" cells under the central government's Department of Telecom.[71] With a number of organisations operating with overlapping mandates, there is some attempt at streamlining with the Joint Intelligence Committee and the Multi-Agency Centre for sharing intelligence inputs between agencies and coordinating action.

Like the IB, RAW and the CBI, the NATGRID and the CMS too are beyond the remit of the Right to Information Act, 2005. [72] The former NATGRID chief has claimed in an interview that the body is subject to "almost 11 structural and procedural safeguards and oversight mechanisms".[73] However, he does not enumerate these safeguards in the interview.

As regards the statutory status of surveillance in India, journalist Saikat Datta traces its origin to early 19th century Imperial Great Britain.[74] The reference here is to the Indian Telegraph Act, 1885 and the Indian Post Office Act, 1898, which allow the police, law enforcement, and intelligence agencies to carry out surveillance. Under the Telegraph Act, central and state governments are empowered to direct the interception of communications "on the occurrence of any public emergency, or in the interest of the public safety" when it is "necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of an offence". The Act also prescribes that the reasons for interception be recorded in writing. According to the Telegraph Rules, orders for interception need to go through a review committee, either at the state or central level, as appropriate. These committees are constituted by the government (state or central) and even constitute members from the executive. The oversight, therefore, is neither external nor impartial.[75] In addition to these two provisions, Section 69(1) of the IT Act allows for similar actions, but for interception and decryption of communication over "any computer resource".

---

[71] Xynou, Maria, "India's Central Monitoring System (CMS): Something to Worry About? — The Centre for Internet and Society", 30 January 2014, https://cis-india.org/internet-governance/blog/india-central-monitoring-system-something-to-worry-about.

[72] Datta, Saikat, "Never Mind the 'Snooping' on Rahul, the Government Is Watching over Even Your Internet Usage", *Scroll.in*, 16 March 2015, https://scroll.in/article/713966/never-mind-the-snooping-on-rahul-the-government-is-watching-over-even-your-internet-usage; See also: Ramanathan, Usha and Ray, Subhadeepta. "A Curious State of Affairs", *Seminar*, no. 641, India 2012 (2013), http://www.india-seminar.com/2013/641/641_usha_ramanathan_et_al.htm.

[73] Agarwal, Vibhuti, "Q&A: NATGRID Chief Raghu Raman", *WSJ* (blog), 29 June 2011, https://blogs.wsj.com/indiarealtime/2011/06/29/qa-natgrid-chief-raghu-raman/.

[74] Datta, "Never Mind the 'snooping' on Rahul".

[75] The controversial 2010 leak of tapped conversations between former corporate lobbyist Niira Radia and various journalists and politicians illustrates the gaps in the surveillance and oversight machinery. At the behest of the country's Income Tax department, Radia's phone was tapped intermittently over a period of two years over 2008 and 2009. In 2010, recordings of the conversations were leaked to select journalists anonymously. Although it caused a significant scandal in political and journalistic circles, government agencies involved in the surveillance did not release information on the reasons of the surveillance and the results of the investigation resulting directly from the phone taps.

The creation of a parliamentary and judicial oversight mechanism over India's intelligence apparatus has seen scattered support and false starts. In 2011, Manish Tewari, a member of the lower house of the Parliament, floated a Bill to introduce safeguards against excesses from the agencies. The Intelligence Services (Powers & Regulation) Bill, 2011 proposed a National Intelligence and Security Oversight Committee and a National Intelligence Tribunal, among other features. The Bill, however, lapsed the following year.[76] Statements by prominent officials have also emphasised the need for oversight. Besides former intelligence officials like Singh and Raman, and legal activists such as Bhushan, former Indian president Hamid Ansari too has made a case for bringing India's intelligence agencies under a legal purview and building a mechanism for accountability. The LP Singh Committee of 1981, formed after the government abuse of intelligence agencies was discovered in the period of the Emergency, also recommended a formal charter of duties for the IB and the CBI. Its suggestions and recommendations were not implemented.[77]

Analysing communication surveillance in India after the Supreme Court judgment declaring privacy a fundamental right, legal scholars Bhandari et al find the Telegraph Rules acutely out of step with developments in modern communication and democratic norms. They find the review process compromised by a conflict of interest (since government bodies both direct and review surveillance orders), and procedural safeguards "fail to constitute a 'fair, just and reasonable' process". They recommend that laws in India that "restrict the right to privacy to be subject to periodic review through a consultative legislative or regulatory process".[78]

### 2.2. Intelligence agencies in Germany

A critique of German intelligence agencies is made possible by the amount of official information available about the agencies' charter of duties, their functions, and the prescribed chains of command for procuring and implementing surveillance orders, in addition to the differentiated functions of the oversight bodies.

With these features alone, the German intelligence community is subject to more parliamentary, judicial, and public scrutiny than the Indian one. Even though the origins of these agencies harken back to either Nazi links or a function of serving Western occupying forces

[76] Bhandari, Vrinda, Parsheera, Smriti, and Rahman, Faiza, "India's Communication Surveillance through the Puttaswamy Lens", *The Leap Blog* (blog), 18 May 2018, https://blog.theleapjournal.org/2018/05/indias-communication-surveillance.html.
[77] Subramanian, K S., "'National Security' for Whom?" *Economic and Political Weekly* 49, no. 25 (21 June 2014): 7–8.
[78] Bhandari, Parsheera and Rahman, "India's Communication Surveillance".

pre-unification[79], there appears to have been an attempt to break from that past through either introducing or amending legislation governing intelligence gathering and streamlining this legislation after the 1980s with the principles of informational self-determination following the landmark Population Census Decision (Volkszählungsurteil) of the Federal Constitutional Court (see section 1). However, commentators and observers within Germany have criticised these agencies for being opaque. The inadequacy of the oversight architecture was highlighted after the Snowden disclosures of 2013 revealed how the German foreign intelligence agency had actively collaborated with the US National Security Agency (NSA).

Intelligence-gathering in Germany today depends chiefly on:

**Table 2**

| **Agency** | **Area of Responsibility** |
|---|---|
| Bundesnachrichtendienst (Federal Intelligence Service or the BND) | Foreign intelligence |
| The Bundesamt für Verfassungsschutz (Federal Agency for the Protection of the Constitution or BfV) | Domestic intelligence |
| Militärischer Abschirmdienst (Military Protection Service or MAD) | Military intelligence |

Formed in 1956, the BND is the foreign intelligence agency, reporting directly to the Federal Chancellery. Its post-war mandate was to closely watch the development of the Eastern Bloc for the Western occupying forces, with staff that drew from the Nazi armed forces.[80] The precursor to the BND was the Gehlen Organisation. Formed in 1946, it was named so after its head, Reinhard Gehlen, the former Wehrmacht Major General. However, the organisation moved quickly through the years to have its activities better defined and streamlined with democratic processes of a modern sovereign state. The first statutory backing for the agency came in 1968 with the introduction of the G10 Act (Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses), which allowed the BND to request and carry out

[79] Krieger, Wolfgang, "US Patronage of German Postwar Intelligence", in *Handbook of Intelligence Studies*, edited by Loch K. Johnson, 1st ed. Routledge, 2007: 91–101. https://doi.org/10.4324/9780203089323.
[80] Ibid.

telecom and post surveillance. By 1990, following the reunification of Germany, the Bundestag enacted the BND Act, giving the body legal backing.[81] The Act, which was amended in 2016, prescribes the ways in which the agency can surveil certain groups of individuals (domestic, EU, or those from a third country) or institutions, and allows it to gather intelligence "about events abroad that are important for the foreign and security policy of the Federal Republic of Germany, if such information can be obtained only in this way and no other authority is responsible for its collection".[82] Its signals intelligence is handled by an internal Technische Aufklärung ("technical investigation") unit, making it subject to the same laws and oversight. This is in contrast with India, where the NTRO is an independent body working on SIGINT for both foreign and domestic intelligence agencies.

Established in 1950 with the West German Parliament passing the Constitutional Protection Act (Bundesverfassungsschutzgesetz or BVerfSchG), the BfV is responsible for domestic intelligence. It answers to the Ministry of the Interior. In contrast to the Indian domestic intelligence agency, there is a conscious institutional separation of the BfV from police powers. This was ensured through the 1949 Polizeibrief, or "police letter", from the military governors of the western occupied zone to the Parliamentary Council drafting the German Basic Law. The idea behind it was to avoid a situation that arose with the National Secret State Police or the Gestapo in Germany from 1933 onwards, where the federal state police mutated into a force that could easily indulge in political espionage.[83] Also in contrast to the IB in India, the BfV has a website designed to inform the public about its tasks and programmes. It distinctly mentions that "the organisation of the BfV is not a secret"[84] and that it may intercept phone and mail communication to collect information on efforts directed against "free democratic basic order" and the security of the state, among other activities.

The MAD has a post-war provenance dating to 1956, when it was established as the Department of Internal Security of the Armed Forces (Innere Sicherheit der Streitkräfte) under the Federal Ministry of Defence by an organisational decree. The MAD describes its functions on its website as similar to the BfV, albeit focused only on efforts targeted at the military and its staff. Although 1956 is considered to be the organisation's date of establishment, it wasn't named the Militärischer Abschirmdienst as it is known today until

[81] Miller, Russell A., "Intelligence Oversight -- Made in Germany", in *Global Intelligence Oversight: Governing Security in the Twenty-First Century*, edited by Zachary K. Goldman and Samuel James Rascoff. New York, NY, Oxford University Press, 2016: 260.
[82] Miller, "Intelligence Oversight", 262.
[83] Goschler, Constantin, and Michael Wala, "Die Geheimnisse eines Geheimdienstes", *Rubin Wissenschaftsmagazin*, Spring 2014, https://www.ruhr-uni-bochum.de/geschichte-bfv/pdf/2014_rubin_verfassungsschutz.pdf.
[84] "The Organisation of the BfV Is Not A Secret," Bundesamt für Verfassungsschutz, accessed 16 July 2019, https://www.verfassungsschutz.de/en/about-the-bfv/tasks/the-organisation-of-the-bfv-is-not-a-secret.

1984.[85] The organisation has undergone a series of restructuring and downsizing efforts after the end of the Cold War and the re-unification of Germany. Statewatch researcher Norbet Pütter finds that before 1990, the MAD did not function under a clear legal basis.[86] That was the year that the Military Counter-Intelligence Service Act, or MAD-Gesetz, was enacted. This law, which was amended in 2005, authorises the MAD "to collect and analyse information during the course of special foreign assignments of the German Federal Armed Forces or during the course of humanitarian missions. Other foreign intelligence gathering is prohibited."[87]

Intelligence oversight in Germany falls under the G10 Commission, Parliamentary Oversight Panel (Parlamentarisches Kontrollgremium or PKGr), and the Independent Committee (Unabhängiges Gremium). The 2016 reforms added an office of the Permanent Intelligence Oversight Commissioner (Ständiger Bevollmächtiger). Besides these, the Federal Data Protection Commission (Bundesbeauftragte für den Datenschutz und die Informationsfreiheit or BfDI) has in the past conducted an inquiry of foreign intelligence activities in the light of the spying scandal uncovered by Edward Snowden.

December 2016 brought reforms to German intelligence law, particularly concerning the gathering of foreign-foreign communication data by the BND, that is, communication where the originating and terminating points are both outside of Germany. The amendment, which introduced conditions for review and oversight for foreign-foreign communications, found its impulse in the 2013 Snowden disclosures, which had exposed German foreign intelligence gathering operations running unhindered by executive and legal checks. The German Parliament's inquiry of the BND over the NSA Affair exposed practices like the agency's intel-sharing agreements with the NSA and a disregard for the right to privacy of communication when it came to correspondence between foreign actors. German and EU institutions were also discovered to have been under US surveillance. The revelation added a touch of apparent duplicity to the response of the Merkel government, which had initially expressed strong and unequivocal displeasure[88] over spying among geo-political allies.
The current post-2016 reform intelligence oversight architecture in Germany, though still criticised as insufficient, includes several bodies at different levels for both ex-ante and ex-post reviews.

---

[85] "Die Geschichte des MAD", Bundeswehr, accessed 26 July 2019, https://mad.bundeswehr.de/portal/a/mad/start/ueberuns/geschichte.
[86] Pütter, Norbet, "Germany The Federal Republic's Security Services from the Cold War to the 'New Security Architecture'", *Statewatch Journal* 19, no. 4 (December 2009): 7.
[87] Gesley, Jenny, "Foreign Intelligence Gathering Laws: Germany", Library of Congress web page, June 2016. https://www.loc.gov/law/help/intelligence-activities/germany.php.
[88] Traynor, Ian, Oltermann, Philip, and Lewis, Paul, "Angela Merkel's Call to Obama: Are You Bugging My Mobile Phone?" *The Guardian*, 24 October 2013, https://www.theguardian.com/world/2013/oct/23/us-monitored-angela-merkel-german.

The Parliamentary Oversight Committee (Parlamentarisches Kontrollgremium or PKGr) is responsible for ex-post review of intelligence policy. The PKGr, which is appointed by the Bundestag, has access to the three agencies. It can inspect their documents and question their officials. The committee with representation from all political parties meets once every three months and recently also started holding annual public hearings.

The PKGr appoints members of the G10 commission, which in turn serves as another important part of the oversight regime. The four-member quasi-judicial committee decides on exceptions to Article 10 of the Basic Law, guaranteeing privacy of correspondence, and on the necessity of surveillance of correspondence. It has the power to reject or accept surveillance orders issued for the BND by the Federal Ministry for the Interior.

The newly instituted three-member Independent Committee (Unabhängiges Gremium or UG) is in charge of reviewing legality and necessity of strategic foreign-foreign communications surveillance. The body is composed of federal judges and appointed by the Federal Cabinet (Bundeskabinett). This panel in turn reports to the PKGr. Additionally, after the 2016 reforms, a position of the Permanent Representative (Ständiger Bevollmächtigter or SB) of the PKGr was introduced. With the same powers and mandate as the PKGr, but in a supervisory role, the position was intended to fill in the functional and administrative gaps in the PKGr's functioning.[89]

In addition to these bodies, the office of the Federal Commission of Data Protection and Freedom of Information (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit or BfDI) is authorised to inspect records of the three agencies to ensure compliance with data protection regulations. Financial audits are taken care of separately with the Federal Court of Audits (Bundesrechnungshof or BRH).

### 2.3. Identifying contrasts and comparisons

The above summarisation of the German and Indian intelligence gathering and surveillance regimes presents an asymmetry—both in terms of available official information and in terms of organisation. This makes a straightforward orange-vs-orange comparison a tricky affair.

The three agencies in Germany have information about chains of command, oversight, and mandates openly available on their websites. In India, while the NIA and the CBI have basic information available on their official websites, the IB and the RAW continue to be under

[89] Müller, Volker, "Deutscher Bundestag - Arne Schlatmann zum Bevollmächtigten des Kontrollgremiums ernannt", Deutscher Bundestag, 10 January 2017, https://www.bundestag.de/dokumente/textarchiv/2017/kw02-schlatmann-pkgr-487768.

wraps. In Germany, information is released through other official channels as well, such as the BND's declassified files released on the 25th anniversary of the fall of the Berlin Wall. Its Indian counterpart, the RAW, has never released declassified documents.[90] The existence of the BND was never meant to be hidden, unlike that of the RAW, which was intended to be a secret agency. [91]

Germany maintains a conscious separation of domestic intelligence and police. In India, however, the opposite is a prominent feature—officers of the IB are known to be drawn from the police service. The abuses stemming from this even prompted the government-constituted L P Singh Committee to recommend reforms in the 1980s, albeit to no avail.[92]

The two countries' responses to the needs of the day for their intelligence services have also been rather different. The two wars in the 1960s and the terror attack of 2008 prompted the addition of new bodies into the Indian intelligence arsenal: the RAW and the NIA, respectively. The Kargil War of 1999 between India and Pakistan was the catalyst for the formation of the NTRO in 2004.[93] In Germany, meanwhile, the evolution has been in terms of powers accorded to the existing agencies and tasks legally permitted for them. When additional bodies were created, they were in the form of an added oversight mechanism.

The Snowden leaks of 2013 provide an illustrative point of comparison between India and Germany. Besides being targets of US surveillance agencies, both India and Germany were also revealed to have been active collaborators of the same. In an internal brief that was part of the 2013 leaks, the NSA described its collaboration with German agencies in areas such as language support and exchanges on military and non-military targets. It also confirms Germany's participation in the 14-member strong Afghanistan SIGINT Coalition (AFSC). The same document describes the BND as "working to influence the German government to relax interpretation of the privacy laws over the long term to provide greater opportunity for intelligence sharing".[94] A similar briefing document describing collaboration with India says the NSA shared "threat warnings, intelligence reports, and lead information" with the RAW. It confirms India's participation in the 10-member strong Sigint Seniors Pacific (SSPAC) collective, where the RAW produced "the highest volume of reports for the SSPAC next to the US and its information has garnered positive feedback from multiple

[90] Raghavan, Srinath, "After 50 Years of RAW, There Are Still No Declassified Documents or an Official History", *ThePrint* (blog), 18 September 2018, https://theprint.in/opinion/why-was-raw-formed-and-what-has-india-learnt-after-50-years-of-its-existence/119811/.
[91] Shaffer, "Unraveling India's Foreign Intelligence", 260.
[92] Subramanian, K S., "'National Security' for Whom?" *Economic and Political Weekly* 49, no. 25 (21 June 2014): 7–8.
[93] Ramanathan and Ray, "A Curious State of Affairs".
[94] "NSA Intelligence Relationship with Germany - Bundesnachrichtendienst (BND)", National Security Agency internal communication, 17 January 2013, https://www.spiegel.de/media/media-34053.pdf.

SSPAC members".[95] The revelations about the BND saw a strong reaction in Germany. It began with the fourth estate kicking into action. The press wrote extensively about the co-operation, leading to the extent of the BND's involvement being officially investigated by oversight bodies. Eventually, when the cracks were discovered after this process, oversight mechanisms were revised. What was a wave in Germany was barely a ripple in India. The press did report on India being one of the targets of US surveillance—something the minister for foreign affairs at the time played down as "not actually snooping".[96] However, the point of India's cooperation with the NSA, by comparison, saw limited coverage and questioning of the government. Tangible official changes in terms of structural changes to the agencies or introduction of judicial or parliamentary oversight were conspicuous by their absence.

Intelligence oversight remains the strongest point of difference between the two intelligence regimes. Civil society, former intelligence officers, and even some public figures in India have pointed to the lack of an oversight mechanism as a lacuna that is out of place in a democracy. Through the Indian lens, the mere existence of checks and balances placed around German intelligence agencies can appear to offer a more robustly preventive alternative. However, German commentators find the local oversight architecture, even post-reform, to be inadequate. A policy brief from the Stiftung Neue Verantwortung (SNV) calls the post-reform German Intelligence Law "a mess".[97] For example, it finds that G10 committee members come from legal backgrounds but do not have judicial powers over the agencies. On the matter of economic espionage, the SNV brief finds that while the practice has been outlawed, the term has not been defined, making execution of the reformed law difficult. Journalists and other observers have found the reforms have now simply legalised the activities that the BND had anyway been carrying out earlier.[98] The civil society group Gesellschaft für Freiheitsrechte has criticised the new foreign surveillance law for not recognising the privacy rights of non-EU citizens. They argue that Section 10 of the German Basic Law grants every citizen anywhere in the world protection from intrusive surveillance.[99] Lawmakers, however, have interpreted this protection as only extending to German citizens.

---

[95] "NSA's Changing Counterterrorism Relationship with India", National Security Agency internal communication, 15 June 2009, https://theintercept.com/document/2018/03/01/sidtoday-2009-06-15-nsas-changing-counterterrorism-relationship-with-india/.

[96] Greenwald, Glenn and Saxena, Shobhan, "India Among Top Targets of Spying by NSA", *The Hindu,* 23 September 2013*,* https://www.thehindu.com/news/national/india-among-top-targets-of-spying-by-nsa/article5157526.ece.

[97] Wetzling, Thorsten, "Germany's Intelligence Reform: More Surveillance, Modest Restraints and Inefficient Controls", June 2017, https://www.stiftung-nv.de/sites/default/files/snv_thorsten_wetzling_germanys_foreign_intelligence_reform.pdf.

[98] Otwinowski, "Tailor-Made Laws".

[99] Spitz, Malte, personal interview, 26 February 2019.

Despite having a relatively sophisticated oversight regime in comparison to India, the German case shows how difficult it is to implement legal boundaries and oversight powers in practice. For instance, the BND's intel-sharing with the NSA took place without any knowledge by the parliamentary overseers. When such incidents are discovered after the fact, as it happened in this case, it leaves little room for corrective manoeuvre. It is for this reason that legal scholar Klaus Gärditz finds both parliamentary and judicial oversight in Germany to be ineffective: "In practice, the parliament can only try to impose a tighter grip on these secretive agencies after something has gone terribly wrong; the parliament lacks a continuously exercised, effective, and routine control. As strong authorization needs strict accountability, and German intelligence law does not entail a preventive judicial control, this blunt desideratum remains a gaping wound in the institutional body of the German intelligence architecture."[100]

Local criticisms notwithstanding, the German oversight structure has not gone unnoticed in India. In its report accompanying the Draft Personal Data Protection Bill, the B N Srikrishna Committee gives an overview of the German model of intelligence oversight, along with remarks on provisions regarding the same in the US, South Africa, and the UK. The Committee makes a strong case, saying, "... it is worthwhile to recognise that all the aforementioned jurisdictions provide some form of inter-branch oversight through a statute. Nothing similar exists in India. This is not just a gap that is deleterious in practice but, post the judgment of the Supreme Court in Puttaswamy, potentially unconstitutional. This is because the Supreme Court has clearly laid down that any restriction of the right to privacy must satisfy three tests: first, the restriction must be by law, second, it must be necessary and proportionate and third, it must promote a legitimate state interest."[101] This concern, however, does not translate into the Bill finally drafted by the committee, where law enforcement and intelligence agencies are given unqualified exemptions when it comes to processing personal data for "security of state" and "exercise of state functions".

Civil society challenges to the intelligence organisations also present a contrast between the two countries. In India, through legal petitions or through the press, the legal basis of the existence and the manner of functioning of Indian agencies have been questioned. We see this with the PIL in the Supreme Court regarding a financial audit of the RAW and the IB, and also the Gauhati High Court case regarding the CBI. In Germany, on the other hand, the questions concern the activities of the agencies and the procedures followed to carry them out, not the very existence of the agencies.

While a preventive intelligence oversight mechanism eludes India, the German one has shown itself to have room for improvement.

---

[100] Gärditz, Klaus, "Legal Restraints on the Extraterritorial Activities of Germany's Intelligence Services", in *Privacy and Power*, ed. Russell A. Miller (Cambridge: Cambridge University Press, 2017), 431, https://doi.org/10.1017/CBO9781316658888.016.

[101] B N Srikrishna Committee, "A Free and Fair Digital Economy", 127.

## 3. Biometric IDs and the potential for profiling

Adding to the steady stream of data ready to be hoovered up, sorted, and tracked are biometric data. When generated and stored as official identity data, they serve as a honeypot not just for commercial interests but also for surveillance agencies. Both Germany and India today have biometric-linked identification systems for its residents and citizens. In India, there is Aadhaar, an ID system where a unique number is mapped to one's identity details like name, address, and so on in addition to biometric data like fingerprints and iris scans. In Germany, not only are the passports biometric-enabled (following an EU-wide move towards biometric passports in 2005), state IDs called Personalausweis too store biometric information.

These two ID systems have operated in very different circumstances. The scale of the Indian one with the sheer number of individuals covered is far larger than the one in Germany. In India, data for the IDs were collected without a data protection legislation in place. In Germany, the same has been subject to legal requirements for data protection. Motivations for the two differ as well. In Germany, the introduction of biometrics to the Personalausweis[102] and the EU-wide adoption of biometric passports[103] were driven by security concerns fomented by the 9/11 terrorist attacks in the USA. In India, efficiency of welfare distribution and delivering essential services was repeatedly cited as an aim of the biometric ID programme.

The deployment of the ID systems in the two countries and the extent and manner of linking services to it also presents points of contrast. Linking to extraneous services is one of the many areas where the possibility of privacy violation occurs. This happens primarily through "function creep"—a phenomenon where a technology built with one end in mind widens in scope to serve others.[104]

Privacy advocates in both countries have raised issue with the use of biometrics as a unique identity. While the unchangeability of biometrics is seen as a security enhancing feature by both governments, the same feature has also raised privacy concerns—since biometric data cannot be altered like a regular password, a breach would mean lifelong effects.[105] It is be-

[102] Noack, Torsten and Kubicek, Herbert, "The Introduction of Online Authentication as Part of the New Electronic National Identity Card in Germany", *Identity in the Information Society* 3, no. 1 (1 July 2010): 95, https://doi.org/10.1007/s12394-010-0051-1.
[103] Cronin, David, "Biometrics – a Passport to Security?", Politico, 22 June 2005, https://www.politico.eu/article/biometrics-a-passport-to-security/.
[104] Schneier, Bruce, "Security and Function Creep", *IEEE Security Privacy* 8, no. 1 (January 2010): 88. https://doi.org/10.1109/MSP.2010.47.
[105] The German interior minister in 2005 defended the use of biometrics in passports as a security enhancing measure. Activists awarded him the Big Brother Lifetime Award as a harsh criticism of the move (see "Germany Introduces Biometric Passports", Deutsche Welle, 1 November 2005,

cause of these reasons that the use and deployment of biometrics as a state ID presents a study in privacy rights. When bundled with welfare services, it introduces sites of contestation regarding the right to access to such services as well.

This chapter will focus on the collection of data by state bodies for identity programmes in India and Germany. In this, it will explore the extent of function creep in both countries and the rights held by citizens when it comes to use of their biometric data. In this, we examine the extent of access of the private sector and the state surveillance machinery to the biometric database.

### 3.1. Aadhaar in India

In India, the Aadhaar programme is an ambitious identity and welfare disbursement programme involving a far-reaching data collection drive by the government. Launched in 2009 with the formation of the Unique Identification Authority of India (UIDAI), the Aadhaar programme assigns a unique biometric-linked identity in the form of a 12-digit Aadhaar number to a citizen or resident of India. The biometrics recorded include iris scans, fingerprints, and a photograph. A citizen can authenticate herself with a service provider using her fingerprints or iris scans. The biometrics are checked against a central database to verify her identity. In other cases, submission of a copy of the "Aadhaar card" —an analogue card—suffices as submission of proof of identity.

According to the 2011 population census, India had a population of 1.2 billion (estimates for 2019 peg it at 1.3 billion). As of 2018, Aadhaar covered over 1.17 billion people in India. The data of those covered by this programme are stored centrally in a Central Identities Data Repository (CIDR). Until 2016, it was also stored state-wise in State Residents Data Hub (SRDH).[106]

Heading the Aadhaar programme since its conception was Nandan Nilekani—Indian billionaire, technocrat, and co-founder of Indian business processing multinational Infosys. The architect of the government ID programme dealing in sensitive data of residents and citizens has been compared with American businessman and politician Michael Bloomberg

https://www.dw.com/en/germany-introduces-biometric-passports/a-1762338.). An Indian right to information activist makes a similar argument in this blog here: Sushil Kambampati, "Aadhaar: The Indian Biometric ID System Has Potential but Presents Many Concerns", *Heinrich Böll Stiftung*, 14 February 2018, https://www.boell.de/en/2018/02/07/aadhaar-indian-biometric-id-system-has-potential-presents-many-concerns.

[106] The government has claimed in court that these state hubs were destroyed in 2016. See: "Biometric Data in State Hubs Destroyed: UIDAI", *The Hindu*, 22 February 2018, https://www.thehindu.com/news/national/biometric-data-in-state-hubs-destroyed-uidai/article22827716.ece.

for his reach and influence.[107] Nilekani, who along with Infosys co-founder Narayan Murthy is often credited with putting India on the global IT services map, was handpicked by the central government to head the Aadhaar project. The politically ambitious businessman quit Infosys to join the UIDAI and remained its chairman until 2014, when he quit again to contest elections. The various conflicts of interest[108] that these successive positions produced were but a small fraction of the issues that plagued Aadhaar.

The Aadhaar programme was envisaged as an accurate technological tool to weed out duplicate beneficiaries for government schemes, particularly with food distribution.[109] However, the government's claims to potential "savings" of 11 billion USD per year with the programme have proven to be sketchy. The government made the claim in the Supreme Court based on a World Bank report.[110] The math and methodology behind the calculation, however, was found to be deeply flawed. The number was found to reflect estimated government expenditure on direct benefit transfers instead of projected savings.[111]

Although it started as a measure for direct benefit transfers, it was gradually made mandatory to link Aadhaar numbers to tax returns, mobile phone numbers, and bank accounts. Linkage was worryingly also encouraged with voter ID cards. Contradictorily, all this while, enrolment into the Aadhaar programme remained voluntary. This linking gave private businesses (such as telecom companies) access to highly sensitive data that was originally meant to be under government control.

While Aadhaar was made mandatory for an increasing number of services, frequent and widespread incidents of inadequate data security and protection practices began to come to light. Bengaluru-based research and advocacy organisation Centre for Internet and Society (CIS) published a report showing how various government departments and ministries had, through their own websites, disclosed 35 million Aadhaar holders' data (Aadhaar numbers, names, addresses, parents' name, etc).[112] This was not a case of unauthorised or malicious

---

[107] Parker, Ian, "The I.D. Man", *The New Yorker*, 26 September 2011. https://www.newyorker.com/magazine/2011/10/03/the-i-d-man.

[108] "Nandan Nilekani Is Part of Every Committee and Group That Is Making Aadhaar Mandatory", *MoneyLife*, 1 October 2013, http://www.moneylife.in/article/nandan-nilekani-is-part-of-every-committee-and-group-that-is-making-aadhaar-mandatory/34677.html.

[109] "Aadhaar will identify genuine beneficiaries of schemes: Centre to SC", *The Economic Times*, 21 March 2018, //economictimes.indiatimes.com/articleshow/63402494.cms?from=mdr&utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst.

[110] "World Development Report 2016: Digital Dividends", World Bank Group, 17 May 2016, https://www.worldbank.org/en/publication/wdr2016.

[111] Drèze, Jean, and Khera, Reetika, "Aadhaar's $11-Billion Question", *The Economic Times Blogs* (blog), 7 February 2018, https://economictimes.indiatimes.com/blogs/et-commentary/aadhaars-11-bn-question/.

[112] Sinha, Amber and Kodali, Srinivas, "Information Security Practices of Aadhaar (or Lack Thereof): A Documentation of Public Availability of Aadhaar Numbers with Sensitive Personal Financial Information", 16 May 2017.

leak without the knowledge or consent of the data handlers. It was in fact a wilful publication of data, with no consideration of it as private or confidential.[113] In fact, after these disclosures were reported, the UIDAI was at pains to claim that an Aadhaar number is not confidential, and "by its very nature" needs to be shared openly. However, a few months and missteps later, the authority pressed upon the people to be "very discreet" with their Aadhaar and other identity documents.[114]

In July 2017, Aadhaar details of subscribers of telecom company Jio were discovered to have been made available on a website called magikapk.com.[115] Next year in January, a crime reporter from a newspaper demonstrated that it was possible to buy access to a software and database to reverse search Aadhaar numbers for personal details of Aadhaar holders. She bought this access with Rs 500 (approximately €6.40) paid over a digital payments app. The negotiation happened on WhatsApp.[116] All through these incidents, the UIDAI maintained that Aadhaar data was safe and that there had been no breach of the CIDR. Instead, it filed a complaint against the crime reporter.

As early as 2012, a petition challenging the constitutionality of the Aadhaar programme was filed in the Supreme Court of India. The petitioners' chief charge was that the programme completely disregarded Aadhaar holders' privacy.[117] The hearings in this matter took place parallel to the routine reports of improper disclosures of Aadhaar holders' data. Meanwhile, the data collection continued, without comprehensive data protection legislation in place. Legal backing for the programme too came during this time. Long after the programme had already been in operation, the Parliament passed the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits, and Services) Act, 2016.[118] According to one of the many contentious provisions of this Act—Section 47—a complaint against the UIDAI could only be filed by the UIDAI. After repeated security scares parallel to the court hearings, the

[113] Ibid.

[114] "Sharing Aadhaar Details Safe or Not Safe? UIDAI Can't Make up Its Mind and Clear Confusion", *India Today*, 12 March 2018., https://www.indiatoday.in/technology/news/story/sharing-aadhaar-details-safe-or-not-safe-uidai-can-t-make-up-its-mind-and-clear-confusion-1187506-2018-03-12.

[115] Bhatia, Rahul, "Exclusive: Police Detain Man in Probe of Alleged Data Leak at India's Jio", *Reuters*, 11 July 2017, https://www.reuters.com/article/us-reliance-jio-cyber-exclusive-idUSKBN19W1E0.

[116] Khaira, Rachna, "Rs 500, 10 Minutes, and You Have Access to Billion Aadhaar Details", *The Tribune*, 4 January 2018, https://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html.

[117] Other petitioners in the case also highlighted the programme's many authentication failures where beneficiaries died of hunger as they could not be authenticated or suffered other hardships. The works of Reetika Khera and Usha Ramanathan are instructive in this regard. This facet of Aadhaar, however, lies outside this paper's focus on privacy and data protection.

[118] This too was mired in controversy as the Act was introduced as a "Money Bill" in the lower house of the parliament. Money bills do not need the assent of the upper house of the parliament, where the BJP—the party that had a comfortable majority in the lower house—was in a minority.

UIDAI introduced "Virtual IDs" in 2018.[119] These were 16-digit numbers that could stand in for Aadhaar numbers during the authentication of a person, with the possibility to generate and revoke them at any point. These, nonetheless, require one to link and register one's mobile phone number with the UIDAI—something that had been a point of contention among privacy campaigners.

During the hearings, petitioners pointed to various leaks of Aadhaar holders' data, the forced linking of biometric data to private services, and the operationally mandatory nature of Aadhaar. With this they reinforced the charge that the programme was violative of privacy. The government's response to these arguments was illustrative on its position on the principle of privacy. First, as discussed in the first section, the Attorney General had argued that the right to privacy did not exist to begin with. In settling this question for once and for all, the country finally recognised privacy as a fundamental right after a separate set of hearings. A second noteworthy argument came up in the right to privacy hearings. This was the charge of elitism against privacy advocates. The Attorney General argued that "an elite few cannot claim that their bodily integrity would be violated by a scheme which serves to bring home basic human rights and social justice to millions of poor households across the country".[120] In the framing of this argument, the concern for privacy was presented as an idea of the privileged that runs counter to the urgency of welfare for the underserved. Others too repeated the charge. Nandan Nilekani has been quoted characterising and dividing those opposing Aadhaar into "four gangs—'the privacy' gang; 'the-rights-of-the-poor' gang; 'the oh-my-god-1984-has-arrived' gang and 'the Luddites', who are scared of technology".[121] A senior editor described Aadhaar opponents as "upper crust, upper class, wine 'n cheese (sic), Netflix-watching social media elite".[122] In this formulation of privacy as an elite privilege, we see the government's reluctance to identify it as an inherent value that deserves protection. It is instead framed as a legitimate and proportional trade-off for welfare of the poor, already vulnerable without losing their right to privacy.

Serving a decision in the Aadhaar case in 2018, the Supreme Court found the programme to be not violative of privacy. The judges also remarked that since the programme had already

[119] "UIDAI Introduces Two-Tier Security to Shield Aadhaar Data", *The Hindu*, 10 January 2018. https://www.thehindu.com/news/national/uidai-introduces-virtual-id-to-address-privacy-concerns/article22411683.ece.
[120] Rajagopal, Krishnadas, "Major Arguments in the Right to Privacy Case", *The Hindu*, 24 August 2017, sec. National. https://www.thehindu.com/news/national/major-arguments-in-the-right-to-privacy-case/article19551038.ece.
[121] Joseph, Manu, "When You Give Your Biometrics to Modi", *Mint*, 7 April 2017, https://www.livemint.com/Leisure/28JmBgGLgWLclLxQtzd9KI/When-you-give-your-biometrics-to-Modi.html.
[122] Gupta, Shekhar, "God, Please Save India from Our Upper Class Aadhaarophobics", *The Print* (blog), 25 September 2018, https://theprint.in/opinion/save-india-wine-n-cheese-aadhaarophobics/27456/.

been rolled out rather extensively, scrapping it altogether would be impractical. However, the court did identify certain sections of the Aadhaar Act as unconstitutional and struck them down. These included Section 47, which only allowed complaints against the UIDAI from the UIDAI itself; a provision to retain authentication data for a period of five years (now it is for a period of six months); and one that required people to mandatorily provide their Aadhaar details to private players in banking and telecommunication in order to be able to use the most basic of services.

However, with a recent amendment to the Aadhaar Act (to account for the Supreme Court's orders), it is still possible for private companies to accept Aadhaar as a know-your-customer (KYC) measure, albeit not mandatorily but when offered by a service user voluntarily. This opens up the field for further Aadhaar documentations. The CIDR continues to function in a manner where the government or the UIDAI may define a later use of the data, defying the principle of purpose limitation in data protection. Aadhaar also continues to be mandatory for disbursement of state benefits.

With KYC links and with records on direct benefit transfers, the possibility of creating an Aadhaar holder's personality profile is real. This concern was also raised by Justice D Y Chandrachud, the lone dissenting judge of the five-judge bench that pronounced the Aadhaar judgment. Justice Chandrachud, who found the entire Aadhaar programme to suffer from "constitutional infirmities", not only makes a reference to the German Volkszählungsurteil (Population Census Decision) of 1983 but also to the country's "decision to reject a centralised database when deploying biometric passports".[123]

Although a minority opinion, Justice Chandrachud's dissenting opinion found international resonance in a similar case in Jamaica. This was in the case of the Jamaican National Identification and Registration Act (NIRA), 2017. Much like the Aadhaar programme, this national ID programme too collected biometric information, offered a unique identification number and a possibility of ID verification. A three-judge bench of the Jamaican Supreme Court unanimously declared it null and void in April 2019. The judgment drew heavily from Justice Chadrachud's dissenting opinion. Writes Justice David Batts in the Jamaican judgment: "From reading the judgments in this case, Dr Chandrachud J, in my respectful view, demonstrated a greater sensitivity to the issues of privacy and freedom that is not as evident in the judgments of the majority or the other judges who delivered concurring judgments. His Lordship had a clear-eyed view of the dangers of a state or anyone having control over one's personal information and generally I preferred his approach to the issue over that of the other judges."[124]

[123] Further details on the official prohibition of creating a centralised database discussed later in chapter.
[124] Robinson, Julian v Attorney General of Jamaica, (Supreme Court of Judicature of Jamaica 12 April 2019).

### 3.2. The German Personalausweis and biometric passports

In Germany, the ecosystem built around biometric-based IDs is much leaner than the one in India in terms of the services linked to them and the data collected for them. The German government collects biometric-based citizen data for issuance of passports and electronic ID cards. All German citizens above the age of 16 are obliged by law to have at least one of these two identity documents. Since 2007, German citizens have been required to submit one fingerprint from each hand when applying for a passport. This was in keeping with EU standards for passports introduced in 2005.

The data collected from a passport applicant—name, photograph, fingerprints, and so on—are recorded on the RFID chip embedded in the passport along with general passport information like date of issuance, date of expiry, and the like. Local passport authorities are obliged to maintain a register of all data except fingerprints. They can store fingerprints only until the passport is handed over to the applicant.[125] Creation of a nationwide database of biometric data on passports is prohibited, as is automated data retrieval, albeit with recently introduced exceptions for law enforcement and intelligence agencies.

Besides the passport, Germans also have the possibility of a personal ID or Personalausweis, which is also electronic and can be used as a travel document within the EU. German electronic IDs, like the Indian Aadhaar, also piloted in 2009 and were eventually officially rolled out in 2010. These credit-card-shaped electronic IDs too, like the passport, store personal data of the cardholder and are linked to biometrics.[126] The matter of this "upgrade" is securitised. In their paper published in the same year as the rolling out of biometric-enabled electronic ID, University of Bremen researchers Torsten Noack and Herbert Kubicek traced the motivation of the introduction of biometrics into the cards to the 9/11 terrorist attack in the USA.[127]

Those in possession of the Personalausweis card have an option where they can, if they so choose, authenticate themselves for online services using a 6-digit PIN. This authentication functions two-way—the holder of the card is also presented with an authorisation certificate from the organisation, website, or service provider asking for authentication. However, since the introduction of the feature in 2010 until 2017, a mere third of the personal ID card

[125] "Passport Act (PassG)", accessed 24 July 2019, http://www.gesetze-im-internet.de/englisch_pa_g/englisch_pa_g.html#p0088.
[126] In addition to this the Aufenthaltstitel, or the ID card for non-EU residents in Germany, also requires the same amount of data to be collected.
[127] Noack and Kubicek, "The Introduction of Online Authentication", 95.

holders had reportedly switched this function on.[128] Since 2017, the electronic ID verification function has been "switched on" by default when one receives one's eID. The government has argued that it is in line with the "Digital Administration 2020" goals of modernisation of e-governance.[129] However, critics have pointed out how this would make security a function of privilege and access. Some of the more secure and higher-quality RFID readers, they say, are more expensive, leaving many vulnerable to attacks.[130] Here one can see the phenomenon of function creep in operation. It can be argued, for example, that users are not being forced to identify themselves to online retailers with the ID's electronic function. But in turning on the function by default, the normal is shifted with a path of least resistance that leads towards it. Nudges are designed to make using the electronic functions easier, while an additional step is created for those who do not want them activated on their cards. Given the lack of popularity of these functions, the number of proactive deactivations over the next few years would provide a conclusive verdict on the government's decision.

Along with these changes, another important amendment to the Personalausweisgesetz (law regulating personal IDs) and the Passgesetz (law governing passports) was also introduced in 2017. Both laws mandate that authorities at the state level keep a register of the details of the identity document for a limited time without storage of fingerprint data, and that no nationwide database of biometric features should be established.[131] Thus far, law enforcement, security, and intelligence agencies were allowed access to data only when these requests were subject to conditions of establishing a basis and were appropriately logged by both the calling and the responding parties. This was changed to allow these bodies unhindered access for automatic retrieval of photographs—an arrangement would be allowed from January 2021 onwards. The logging would only be required from the calling side. Automated retrieval, which was earlier only allowed under extraordinary circumstances of not being able to reach any of the local offices storing the information, is now unhindered by these conditions. Criticising the move, German newspaper taz explained the rationale of this move as that of maintaining secrecy of intelligence and investigative

[128] "Neues Personalausweis-Gesetz: Bundestag erlaubt massenhaften Zugriff auf Passfotos", *Spiegel Online*, 19 May 2017, sec. Netzwelt, https://www.spiegel.de/netzwelt/netzpolitik/elektronischer-personalausweis-eid-bundestag-erlaubt-zugriff-auf-ausweis-fotos-a-1148394.html.
[129] Die Bundesregierung, "Sicherer Identitätsnachweis im Netz", 15 July 2017, https://www.bundesregierung.de/breg-de/aktuelles/sicherer-identitaetsnachweis-im-netz-388084.
[130] Dachwitz, Ingo, "Im Gesetz zum elektronischen Personalausweis versteckt sich ein automatisierter Abruf für Geheimdienste [Update]", *netzpolitik.org*, 24 April 2017, https://netzpolitik.org/2017/im-gesetz-zum-elektronischen-personalausweis-versteckt-sich-ein-automatisierter-abruf-fuer-geheimdienste/.
[131] "Act on Identity Cards and Electronic Identification (Personalausweisgesetz, PAuswG)", accessed 24 July 2019, http://www.gesetze-im-internet.de/englisch_pauswg/englisch_pauswg.html.

work.[132] Former Federal Commissioner for Data Protection and Freedom of Information Peter Schaar called it a "Big Brother Law".[133] Organisations like the Chaos Computer Club (CCC) have criticised the amendment saying that it would effectively create a nationwide database of biometric photos with intelligence and security agencies. It is for this reason that digital rights activism and advocacy organisation Gesellschaft für Freiheitsrechte has filed a constitutional complaint against the amendment along with other petitioners.[134]

This amendment must be seen in the light of Germany trialling and deploying facial recognition technology in public areas and at border controls.[135] A trial for a facial recognition-powered video surveillance system has already been run at Berlin's Südkreuz station.[136] Coupled with the amendment for automated retrieval for photographs, a person's face would be rendered as de facto tracking data.

The expansion of surveillance powers via the ID laws together with reduced logging requirements illustrates a worrying trend where the secrecy, efficiency, and speed of the intelligence and investigating agencies trumps their accountability. The creation of an implicit, functional possibility of a national database of biometric photos as an exception to the current law is an example of securitisation in this domain.

### 3.3. Identifying connections and contrasts

There is a clear distinction to be seen in the nature of state powers, entitlement, and transparency that the Indian and German governments envisage with the authentication procedures of their electronic ID cards. The service provider (or the "relying party," as it is called in Germany) in India is not required to furnish a certificate of authorisation to the person authenticating herself, which happens to be a norm in Germany.

[132] Rath, Christian, "Zugriff auf Passfotos aller Bundesbürger: Fotoalben für Geheimdienste", *Die Tageszeitung: taz*, 26 April 2017, sec. Politik. https://taz.de/!5404643/.
[133] "Neues Personalausweis-Gesetz", *Spiegel Online*, 19 May 2017, sec. Netzwelt, https://www.spiegel.de/netzwelt/netzpolitik/elektronischer-personalausweis-eid-bundestag-erlaubt-zugriff-auf-ausweis-fotos-a-1148394.html.
[134] "Automatisierte Passbildabfrage – GFF – Gesellschaft für Freiheitsrechte e.V.", 6 December 2018, https://freiheitsrechte.org/automatisierte-passbildabfrage/.
[135] The deployment at EU border crossings has been advertised as an attractive "quick, simple, time-saving" option. "EasyPASS - Was Ist EasyPASS?", accessed 22 October 2019, https://www.easypass.de/EasyPass/DE/Was_ist_EasyPass/home_node.html.
[136] Delcker, Janosch, "Big Brother in Berlin", *Politico*, 13 September 2018, https://www.politico.eu/article/berlin-big-brother-state-surveillance-facial-recognition-technology/.

The treatment of numbers linked to the IDs also shows a marked difference in the two countries. While the Aadhaar number is linked to a person's identity in India (required to be cited as such in tax returns, for example), the German Personalausweisgesetz prohibits the use of the unique serial number on the card as an identifier. In comparison to India, the encouragement of the electronic ID in Germany did not depend on making it mandatory to be linked to various services. Data storage requirements in Germany also differ with India maintaining a central repository in the form of the CIDR and the German law expressly prohibiting such a database.

These differences illustrate an essential difference in the state-citizen relationship in the two countries. The Indian state can be seen to take on the position of a top-down provider, the functions of which are strongly dependent on asserting and maintaining authority and having a measure of power—either through possession of data or through unilaterally introducing compulsory measures. The German state, on the other hand, appears to put the citizen on a relatively even footing, allowing her transparency from the other end in her electronic transactions as well, which by themselves remain optional.

However, in both countries, we do see function creep widening the scope of biometric ID systems. In India, it broadened to private sector services for a while before being contained by the court. Outside of welfare services, Aadhaar is still required for filing taxes. In Germany, the 2017 amendment opened biometric IDs up to law enforcement agencies. Function creep of this sort significantly raises the risk of profiling. Eminent German jurist and data protection expert Spiros Simitis made this observation as far back as 1987. "Experience has shown that national identification systems quickly become integrated into the private sector, either, as in the case of employees, because of legislative requirements, or because of peculiar interests of private organizations ... The more widespread the use of the identifier, the better the chances of creating an exhaustive information base through an electronic linkage of the files", he wrote. These are the very concerns raised by civil society members and local observers today in both Germany and India when it comes to widespread deployment of biometric IDs.

The Supreme Court of India privacy judgment of 2017 acknowledges the risks of government excesses with the use of citizen data, particularly profiling. "The growth and development of technology has created new instruments for the possible invasion of privacy by the State, including through surveillance, profiling, and data collection and processing", says the unanimous judgment from the nine-judge bench.[137] Referring to the GDPR to define profiling, the judgment goes on to qualify its acknowledgment of risks posed by state surveillance and profiling by adding: "Such profiling can result in discrimination based on religion, eth-

[137] Justice K Puttaswamy (Retd) and Another v Union of India (Supreme Court of India, 24 August 2017).

nicity and caste. However, 'profiling' can also be used to further public interest and for the benefit of national security."[138] This opens the door to potentially securitise the use and proliferation of biometric IDs.

In India, there was an opportunity to strengthen state accountability against such state excesses with the Draft Personal Data Protection Bill, 2018. It provides Indian citizens with a range of protections when it comes to misuse of data from body corporates. However, it allows collection and processing of data by the government under broad exceptions. In Germany, on the other hand, the recent spate of legalisation of intelligence activities and an inclination towards building what has effectively been interpreted to be a national database of citizens, indicates that the approach is gradually changing here as well, albeit with a healthy dose of pushback from civil society organisations.

[138] Ibid.

## 4. GDPR and the BDSG-Neu vs the Draft Personal Data Protection Bill: Comparing user rights, government obligations, and the conditions of data transfer

On 24 May 2019, Stiftung Datenschutz held an event in Berlin to mark one year of the Global Data Protection Regulation (GDPR). It had, among scholars, lawyers, and politicians, the German Federal Data Protection Commissioner Ulrich Kelber in attendance. The day began with a discussion on GDPR as a regulatory "global export". The GDPR has indeed had legal consequences beyond EU borders, requiring data controllers and data processors to comply with its provisions regardless of where they are incorporated, as long as they deal with data of EU citizens and residents. Internet companies in the US, particularly giant corporations like Google and Facebook, have been its most-watched targets. Kelber pointed to California and its California Consumer Privacy Act (CCPA), as well as the recent developments in data protection legislation in Mexico and Brazil[139] as a testament to the GDPR becoming an international standard.

In India, the Supreme Court judgment of August 2017, which recognised privacy as a fundamental right, makes several references to the GDPR when referring to the right to be forgotten, defining profiling, and laying out restrictions to the right to privacy. Justice Sanjay Kishan Kaul even went so far as to say that in India's drafting of suitable data protection legislation, the GDPR "may provide useful guidance".[140] The BN Srikrishna committee, tasked by the central government with formulating the Draft Personal Data Protection Bill, looked closely at the GDPR. A report that accompanied the Bill, which was released in 2018 after the GDPR was enforced, mentions the EU law 85 times. The report, which offers an insight into the committee's deliberations and concerns while drafting the Bill, says that although it learns from global best practices, it is mindful of India's specific context and in that it "ploughs its own furrow" when formulating a law. The regulatory architecture it proposes—with supervisory authorities, data protection authorities and data protection officers—is similar to the one under the GDPR. It proposes a right to be forgotten, right to correction, and right to confirmation and access—which at a cursory reading would appear to be modelled on the GDPR. This chapter closely examines these provisions to discover how they actually differ in principle and also offer a different practical application.

[139] In 2018, Mexico acceded to the Convention 108—an international treaty that protects individuals from the abuse of automated data processing. It also regulates cross-border data flows. Brazil approved its Data Protection Law in 2018. It is scheduled to come into force in February 2020

[140] Justice K Puttaswamy (Retd) and Another v Union of India (Supreme Court of India, 26 September 2018).

The EU has already been in official contact with India regarding its Draft Personal Data Protection Bill. In September 2018, the European Commission's unit for International Data Flows and Protection wrote to India's Ministry of Electronics and Information Technology (MeitY) with comments on the publicly released Draft Bill. While congratulating the country for taking this significant step towards data protection, it also pointed out various ways in which the Bill could benefit from strengthening provisions. Besides data subject rights, data localisation, and exemptions for the state, the Commission also highlighted the issue of the independence of the supervisory authority, which, under the Draft Bill, can be issued directions as well as funds from the central government.[141]

Operational architectures for data protection laws differ significantly in Germany and India. In Germany, one must take into consideration both the EU-wide GDPR and the local Bundesdatenschutzgesetz-Neu, or BDSG-Neu (Federal Data Protection Act-New), which is harmonised with the larger regulation. In addition to this, the 16 German states also have state legislation with state-level data protection laws (Landesdatenschutzgesetz or LDSG).

Legal consultant and professor of data privacy law Lothar Determann has argued that in practice this has meant repetition of clauses in local implementation laws with a difficult-to-understand legal matrix for the layperson.[142] However, data protection commissioner for the state of Schleswig-Holstein Marit Hansen finds the current arrangement works to the advantage of the aggrieved individual seeking legal recourse. She says that while there are indeed several layers of legal compliance, it is only for the administrators, as the aggrieved individual is free to approach any data protection authority. She finds that since various procedures that have been laid down at different levels, "there are mostly solutions that fit the demands".[143]

Eventual effects notwithstanding, the intent of the GDPR was to update and streamline data protection across Europe.[144] Its precursor is found in the Data Protection Directive of 1995 (adopted 1998), which laid down many of the rules and principles we recognise today, such as consent of the data subject when processing data, purpose limitation, and assurance of adequate data protection when transferring data to "third countries" or countries outside

[141] Gencarelli, Bruno, "Submission on Draft Personal Data Protection Bill of India 2018 by the Directorate-General for Justice & Consumers to the Ministry of Electronics and Information Technology (MeitY)", European External Action Service, 19 November 2018, https://eeas.europa.eu/delegations/india/53963/submission-draft-personal-data-protection-bill-india-2018-directorate-general-justice_en.

[142] Translated and paraphrased from a public talk at the Datentag by Stiftung Datenschutz in Berlin, 24 May 2018.

[143] Hansen, Marit, personal interview, 18 April 2019.

[144] "European Commission Press Release - Agreement on Commission's EU Data Protection Reform Will Boost Digital Single Market", 15 December 2015, https://europa.eu/rapid/press-release_IP-15-6321_en.htm.

the EU. It is now replaced with the GDPR, a regulation that had been seven years in the making, to better respond both to the new geopolitical issues emerging with increased use of data gathering and digital technologies in business and governance.

In India, in the absence of separate and exhaustive legislation, data protection is governed by a set of rules introduced via an executive order under the Information Technology Act, 2008. These are the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. These Rules, however, are limited in only regulating the conduct of "body corporates" and have been noted for excluding "natural persons and most public entities from its purview".[145] The Draft Personal Data Protection Bill of 2018 is more exhaustive in acknowledging and defining the rights of an individual.

In India, with the recognition of privacy as a fundamental right, individual freedoms came into sharp focus in the national debate, and it was clear that the state or corporations could not ride roughshod over individual interest. In the EU, bolstered by the GDPR (though he was active even before it), Austrian activist Max Schrems took on a tech behemoth like Facebook on the basis of an individual complaint. To explore this dynamic of the individual within the larger legal rubric of data protection further, this section will focus on the individual rights defined in the BN Srikrishna Committee's Draft Personal Data Protection Bill (the Draft Bill) of 2018 and the relevant comparable provisions in the GDPR or BDSG-Neu (whichever is applicable in context). It will also compare the contentious data localisation provisions and the exceptions to data protection obligations afforded to state bodies and government agencies, which have often proven to be the potential sites of violation of individual rights.

### 4.1. Objectives

The Draft Bill lays out its objectives as those of protecting the "autonomy of individuals in relation with their personal data, to specify where the flow and usage of personal data is appropriate, to create a relationship of trust between persons and entities processing their personal data, to specify the rights of individuals whose personal data are processed, to create a framework for implementing organisational and technical measures in processing personal data, to lay down norms for cross-border transfer of personal data, to ensure the accountability of entities processing personal data, to provide remedies for unauthorised and harmful processing, and to establish a Data Protection Authority for overseeing pro-

[145] Chaturvedi, Aditi, "GDPR and India", Center for Internet and Society, 17 October 2017, https://cis-india.org/internet-governance/files/gdpr-and-india.

cessing activities." The text of the GDPR also lays down rules "relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data"; it also spells out what it really seeks to protect with data protection. "This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data", says Article 1 of the GDPR. There are some similarities in the two chief subjects addressed here—fundamental rights and cross-border data transfers.

Both the Draft Bill and the GDPR place the individual at the centre of their respective frameworks, guarding their "autonomy" (Draft Bill) and their "fundamental rights and freedoms" (GDPR).

As concerns data transfers, the Draft Bill, in its objectives, takes a stance of protecting against potential harm. In contrast, the GDPR characterises its objectives with data transfers as not protective but facilitative of "free movement" of personal data. That is, of course, as far as data flow within EU borders is concerned. This dovetails with the objectives of the European Single Market.[146] However, as we see with further provisions of the Regulation concerning data transfers to third countries, strict restrictions and adequacy requirements apply. The objectives of both the Bill and the GDPR make clear that they seek to establish procedural norms and safeguards for the flow of data—the Bill in a detailed manner and the GDPR in a succinct one.

Privacy and big data expert Bart van der Sloot sees rights concerning free expression or freedom of religion as those that vary from country to country with varying "traditions and cultural standards". In this context, he observes the data protection regime extending across the EU as making the right to data protection a more international one. He finds that data protection has a "particular international and transnational character, due to cloud computing and other modes of cross-border data transmission". He warns that "by undermining the diversity in national approaches, the democratic legitimacy of the right to data protection may be undermined as well".[147] While Sloot's observations concern the regulation in the EU, the extension of the values to countries like India can be seen to produce similar potential frictions.

[146] A European Commission arrangement ensuring the free movement of goods and services within the EU.

[147] Van der Sloot, Bart, "Do Data Protection Rules Protect the Individual and Should They? An Assessment of the Proposed General Data Protection Regulation", *International Data Privacy Law* 4, no. 4 (1 November 2014): 319–20. https://doi.org/10.1093/idpl/ipu014.

### 4.2. Rights of the data subject

The individual whom the personal data belongs to or is associated with is identified as a "data subject" under the GDPR and a "data principal" under the Draft Bill. What the GDPR calls the "data controller", that is, a body, organisation, or person that decides the purposes and means of processing data, is called the "data fiduciary" in the Draft Bill and is defined similarly as well. The rights for the individual recognised by both use a similar terminology.

***Access.*** Under Article 15 of the GDPR and Section 24 of the Draft Bill, individuals have a right to access their data from a data controller/fiduciary. Chapter three of the GDPR lists the various kinds of information that the individual may receive in addition to the personal data itself. These include purposes of processing, contact details of data protection officer where applicable, categories of personal data processed, period of storage, existence of automated decision-making along with an explanation of the rights to lodge a complaint. Data controllers are prescribed to share the same set of information (similarly worded in the Draft Bill) when requested, in Section 8 the Draft Bill under Chapter II on "Data Protection Obligations," with an addition of a "procedure for grievance redressal".

Under the Draft Bill's "Right to Confirmation and Access" in Section 24, an interesting contrast to the GDPR's Article 15 emerges. The GDPR grants the individual the "right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data" in addition to other information regarding the processing of the same. The Draft Bill on the other hand grants the individual a right to obtain "a brief summary" of personal data processed and "a brief summary" of the processing activities therein. This seems to leave wiggle room for data controllers to withhold information under a right to access request.[148]

The EU Commission in its comments on the Draft Bill—submitted to the Indian Ministry of Electronics and Information Technology (MeitY)—commented on this requirement saying that the law could be more specific and instead entitle an individual with a right to access

[148] It is worth mentioning here that in Europe, GDPR Article 15 was received by small and medium enterprises (SMEs) as one of the requirements that increased administrative burden on them. Consultancy firms such as Deloitte and law firms such as Taylor Wessing published guidelines and blog posts on GDPR compliance for SMEs focusing on the documentation burden. While the Draft Bill's Section 24 may provide wiggle room for bigger corporate entities, smaller businesses may find their burden diminished. In a Council of the EU document aimed at the GDPR review in 2020, one can find such arguments from countries like Germany and Lithuania mentioning the administrative burden of documentation for SMEs: "Preparation of the Council Position on the Evaluation and Review of the General Data Protection Regulation (GDPR)-Comments from Member States", General Secretariat of the Council of the European Union, 9 October 2019, https://data.consilium.europa.eu/doc/document/ST-12756-2019-REV-1/en/pdf.

her data in full.[149] However, the application of the right in Europe itself seems to have room for a similar interpretation. In a December 2018 report, the Hessian Commissioner for Data Protection and Freedom of Information commented on the scope of the right to access, saying that in the right to obtain a "copy" of one's data from a data controller, the term "copy" should be interpreted as "a summary of the personal data structured in a meaningful way".[150] This interpretation appears to be in line with that of the B N Srikrishna Committee. However, the Labour Appeals Court of Stuttgart and the Appeal Court of Cologne have interpreted the right more strictly. [151] It would be interesting to watch both Indian parliamentarians and EU courts interpret this right in the light of international developments and local needs.

***Correction.*** Article 16 of the GDPR, in a succinct paragraph, gives a data subject "the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her" and also "the right to have incomplete personal data completed, including by means of providing a supplementary statement". The Indian equivalent in the Draft Bill with the right to correction under Section 25 is longer and qualified. It also makes procedural prescriptions for such a case where the data fiduciary and the data principal may disagree on the correction/completion/updation. In case the fiduciary does not agree with the data principal's request, it must provide her with justifications for turning down her request. When the justification is not to the principal's satisfaction, the fiduciary is obliged to indicate the disputed nature of the data. All corrections/completions/updations must be communicated to the processors as well.

To find similar procedural prescriptions in the German context, one must read the section on correction in conjunction with other provisions. Article 12 (4) of the GDPR asks controllers to communicate lack of action on an information request along with reasons thereof to the data subject. In case of a further dispute, Section 44 of the BDSG-Neu allows the data subject to initiate proceedings against a controller for violating her rights under the GDPR, where the court may be in her place of habitual residence.

While these are merely procedural differences, there is another curious point of contrast. In the Indian Draft Bill, the opening paragraph on the right to correction introduces what can

[149] Gencarelli, "Submission on Draft Personal Data Protection Bill of India 2018".
[150] Elteste, Ulrike, Van Quathem, Kristof, and Oberschelp de Meneses, Anna, "German Supervisory Authorities Issue Guidance on Data Subject Rights", *Inside Privacy*, 12 July 2019, https://www.insideprivacy.com/international/european-union/german-supervisory-authorities-issue-guidance-on-data-subject-rights/.
[151] "German Court Decides on the Scope of GDPR Right of Access", *Inside Privacy*, 8 August 2019, https://www.insideprivacy.com/international/european-union/german-court-decides-on-the-scope-of-gdpr-right-of-access/.

be interpreted as a qualification. It says, "Where necessary, having regard to the purposes for which personal data is being processed, the data principal shall have the right to obtain from the data fiduciary processing personal data of the data principal—

(a) the correction of inaccurate or misleading personal data;

(b) the completion of incomplete personal data; and

(c) the updating of personal data that is out of date."

As the Draft Bill does not define what comprises necessity in "where necessary", it creates uncertainty. In the European context, while there is room to implement exceptions to the application of these rights (discussed later in this chapter), it does not include a necessity requirement within the phrasing of the right itself.

With the bundling of grievance redressal mechanisms as well as procedural specifications in case of a dispute in the right to correction, the Indian drafting of the right to correction appears to be more comprehensive. It would, however, benefit from clarifying the basis of necessity as laid down in the opening line. The European equivalent offers a leaner and more straightforward phrasing.

***Right to be forgotten and the right to erasure.*** This is among the most discussed and known rights globally, coming into the spotlight as it did with the Google Spain case of 2014. This was two years before the adoption of the GDPR in 2016.

Under Article 17 of the GDPR, it is framed as "right to erasure (right to be forgotten)", whereas in the Draft Bill, it is termed the "right to be forgotten". Given its genesis in the Google Spain decision of 2014,[152] there are two things at play here: First is the erasure of data that are no longer relevant. Second is the removal of links to said data from search engine results.

The EU law allows for the erasure of data as well as for the "delisting" of links from search engine results. "Delisting" is when, for example, a news report would continue to be hosted

[152] This was the Google Spain v AEPD and Mario Costeja González decision of the European Court of Justice in 2014. It involved lawyer Mario Costeja González, news of whose property being auctioned off to settle debts was published in the newspaper La Vanguardia. Having settled the debt, González requested that the newspaper delete the story, as it was no longer relevant. When that did not work in his favour, he sued Google Spain, saying they must remove links to the news report, arguing that it was no longer relevant, and yet, Google searches for his name continued to throw up results of the auction. The court upheld González's complaint in this regard (though not with regard to the newspaper).

on a news website, but the link to it would not appear in the results of a search engine. Section 17(2) essentially talks of delinking when it says that "the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data." The Draft Bill does not make any reference to delisting links to information that a data principal may deem unnecessary, outdated, or irrelevant. Section 27 of the Draft Bill allows for the "restriction or prevention of continuing disclosure of personal data by a data fiduciary" when it is no longer necessary and has served its purposes, when consent has been withdrawn, and when such an action is unlawful.

Although there isn't a reference to delisting, there is a reference to publicly available information. Section 27(3) in the Draft Bill lays out the conditions against which an "Adjudicating Officer" should assess the legitimacy of a right to be forgotten request. Among the five conditions, there are "the role of the data principal in public life" and "the relevance of the personal data to the public". This issue of balancing the right to be forgotten with the right to be informed and/or freedom of information came up in the Google Spain decision, and has been addressed in the GDPR as well. Article 17(3) of the GDPR too offers derogations to the right on the counts of "exercising the right of freedom of expression and information" and "archiving purposes in the public interest, scientific or historical research purposes or statistical purposes", among others. There is an additional derogation under Section 35 of the BDSG-Neu. It says that "in the case of non-automated data processing erasure would be impossible or would involve a disproportionate effort due to the specific mode of storage and if the data subject's interest in erasure can be regarded as minimal, the data subject shall not have the right to erasure and the controller shall not be obligated to erase personal data".

While the Google Spain decision was widely criticised for its lopsided view of the right to be informed against right to be forgotten,[153] the provisions for now balancing the two appear to leave room for further case law to develop differently.

We see here both jurisdictions address the issue of user data being deleted once the said user leaves a service or revokes consent. However, sections on publicly available information offer up a point of difference where the European regime has a specific mention of delisting links from search engine results—something the Indian Draft Bill omits. Both, however, do prescribe checks and balances when making exceptions to a right to be forgot-

[153] "Google Spain SL v. Agencia Española de Protección de Datos", *Harvard Law Review* 128, no. 2 (10 December 2014), https://harvardlawreview.org/2014/12/google-spain-sl-v-agencia-espanola-de-proteccion-de-datos/.

ten request. The applicability of the same continues to be refined with case law, as we saw with the recent European Court of Justice ruling in September 2019, saying that the right to be forgotten as prescribed in the GDPR would only apply within the EU, and a search engine need not limit results outside of that jurisdiction.[154]

***Right to data portability.*** Both in the GDPR and the Indian Draft Bill, the right is named the same way, and both lay down the right of the data subject to receive personal data "in a structured, commonly used and machine-readable format". In both cases, a data subject has the right to transfer her personal data from one controller/fiduciary to another, and the right is only applicable for data processed through automated means and where it is technically feasible to transfer it. The exemptions to transfer in both cases are also similar. In the Indian Draft Bill, the right does not apply where the processing is "necessary for functions of the State" or where it is necessary for legal compliance. In the GDPR, the exemption is for cases where processing is necessary "for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller". An additional caveat from the GDPR under Article 20(4) is that the exercise of the right to portability must not "adversely" affect the exercise of any other right.

However, they differ in the kinds of data they recognise for the purposes of porting and in the manner in which they recognise these kinds of data.

Article 20 of the GDPR identifies data that may/may not be ported as "personal data concerning [a data subject], which he or she has provided to a controller". Section 26 of the Indian Draft Bill, on the other hand, qualifies the kinds of data that may/may not be ported as data provided by the data principal to the fiduciary, data generated in the course of goods or services provision, and any data that "forms part of any profile on the data principal or which the data fiduciary has otherwise obtained".

On first look, the GDPR appears to only concern itself with regulating the porting of data that has been explicitly provided by the subject to the controller. The Indian Bill, on the other hand, also accounts for data generated about the subject in the course of processing activities.

The legal scholars, and privacy and technology law experts Paul De Hert et al have interpreted the data types under Article 20 in an "extensive" manner, that is, as inclusive of data generated by the controller in the course of processing and data otherwise obtained as

[154] Chee, Foo Yun, "You Have the Right to Be Forgotten by Google - but Only in Europe", *Reuters*, 24 September 2019, https://www.reuters.com/article/us-eu-alphabet-privacy-idUSKBN1W90R5.

well.[155] To do this, they rely on Recital 68, which says "the right to data portability should apply where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract". They also rely on the European Data Protection Supervisor recommendation that the right to data portability have "a wide scope of application, and not only be applied to the processing operations that use data provided by the data subject". They also point to the Working Party 29 recommendation that the phrase "provided by" be interpreted broadly. One is yet to see how it is applied in case law. The Indian Draft Bill defines far more clearly the kinds of data that are valid for porting.

### 4.3. Cross-border transfer of data and data localisation

The Indian Draft Bill proposes that data controllers store a serving copy of personal data they have in their possession on servers located within India. This has generated much comment on ease of setting up and maintaining businesses both within the country and without. More importantly, there have been concerns about what this move would mean for domestic surveillance and the individual's right to privacy. The GDPR, on the other hand, introduces conditions for transfer of data to third countries, but unlike India, has no explicit condition to store data within EU borders. Nonetheless, the terms of transferring data across borders has been at the centre of legal and economic discussions with Schrems challenging data transfers from Facebook Ireland to the social media conglomerate's parent company in the US. Here too, surveillance concerns were raised, albeit the potential surveillance of European citizens by US agencies.[156]

Articles 44-50 of the GDPR on "Transfers of personal data to third countries or international organisations" essentially set down terms of transfer of data—subject to consistency when done to a country within the Union, and subject to data protection standards when transferred to a country outside of the European Union (third country). Recognising a country as fit for free flow of data with a data adequacy agreement (as laid down in Article 45) takes into account several aspects. These include factors as far-ranging as respect for human rights to the presence of a data protection supervisory authority. As of August 2019, the EU had adequacy agreements with 13 countries.

---

[155] De Hert, Paul, Papakonstantinou, Vagelis, Malgieri, Gianclaudio, Beslay, Laurent, and Sanchez, Ignacio, "The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services", *Computer Law & Security Review* 34, no. 2 (April 2018): 193–203, https://doi.org/10.1016/j.clsr.2017.10.003.

[156] "CJEU Hears Case on EU-US Data Transfers (Standard Contractual Clauses and Privacy Shield)", *Noyb.Eu*, accessed 19 August 2019. https://noyb.eu/cjeu-case/.

Other legal means for cross-border transfer of data to third countries include: binding corporate rules for an international group of enterprises and/or their business partners when engaged in joint economic activity (Article 47), Commission-approved codes of conduct or certification mechanisms (Article 46), or via derogations such as the need for performance of contract or when the data subject herself consents to the transfer of data (Article 49). Data requests resulting from court decisions can be complied with by relevant mutual legal assistance treaties (MLATs) between concerned countries (Article 48).

The Indian Draft Bill proposes a more stringent regime. Apart from adequacy conditions, Section 41 of the Draft Bill mandates that the data protection authority may approve standard contractual clauses. Much like the GDPR, it may also lay down conditions for transfer. However, Section 40 introduces strict restrictions for the same. Section 40(1) asks every data fiduciary to "ensure the storage, on a server or data centre located in India, of at least one serving copy of personal data to which [the] Act applies". It also requires that certain categories of "critical personal data" shall only be processed in a server of data centre located in India. These categories of "critical personal data" aren't defined in the Bill but are left to the central government to notify. The government is also given an opening to define exceptions to these clauses based on "necessity or strategic interests of the State".

Data localisation in India has been presented as a way for the government to work around the slow MLAT processes in case of cross-border crimes or other legal violations that may happen on foreign-owned social media or technology platforms. In its report accompanying the Draft Bill, the Srikrishna Committee cites a need to "reduce reliance on the MLAT request regime"[157] as one of the motivations to introduce these conditions.

Noting that eight out of the top 10 most visited websites by Indians are US-based, the Committee finds that "law enforcement bodies often need to gain access to information that is held and controlled by data fiduciaries. As a result of this, it is important for the law to acknowledge the importance of quick and easy access to information to effectively secure national security and public safety. A requirement to store personal data locally would boost law enforcement efforts to access information required for the detection of crime as well as in gathering evidence for prosecution. This is because it is easier for law enforcement agencies to access information within their jurisdiction as compared to awaiting responses to requests made to foreign entities which store data abroad." The Committee also realises that the long-term solution to this lies not in data localisation but in modernising current procedures to respond better to a digitally connected world. "However, it is advisable that in the future, nation states should strive towards harmonisation to create an enforcement regime that provides for effective information sharing", says the Committee re-

[157] B N Srikrishna Committee, "A Free and Fair Digital Economy", 96.

port.[158] Interestingly, their reasoning for this proposal mirrors that of the Constituent Assembly when rejecting privacy as a fundamental right (see section one of report). Here too the practical and operative ease of law enforcement is a key interest that trumps other concerns.

The GDPR prescribes a set of rules and conditions that must be met for the transfer (to third countries) of personal data either under processing or intended for processing. Contained in Chapter 5 of the Regulation, these include, among others, an adequacy decision from the European Commission deeming third countries or international organisations meeting the EU data protection requirements; contractual and other kinds of safeguards in the absence of such a decision; and competent supervisory authority-approved binding corporate rules. There is no explicit requirement to store a "serving copy" of personal data within EU borders as we see in India. However, the transfer conditions have been seen as restrictive by some quarters. A research report on data localisation from the Leibniz Information Centre for Economics, in cooperation with the European Centre for International Political Economy, warned that "GDPR reform could lead to a stoppage of cross-border data flows from the EU to important data processing countries such as the US and India, which are deemed to have adequate data privacy safeguards in place under the EU's current regime".[159]

While the EU regime has raised concerns regarding data flows, the Indian data localisation proposal has provoked unease regarding individual rights. In their analysis of India's data localisation proposal, Rishab Bailey and Smriti Parasheera point out how "[p]hysically locating all data within the territory of a state leads to a significant increase in the capacity of law enforcement agencies to access that information, and consequently surveil domestic residents". In terms of alternative mechanisms, they point to the Telecom Regulatory Authority of India's (TRAI) 2017 recommendations on cloud services, where it is suggested that MLATs signed with various countries be made more comprehensive. The TRAI has also suggested the use of the US CLOUD Act to obtain data on Indians from US companies. [160]

Currently, both countries have a limited localisation regime. India has a localisation requirement for financial and payments data. Germany enforces the same with telecommunications metadata. However, when it comes to the overarching legislation governing data flows, India has shown a stronger bent towards protectionism with the regime proposed under the Draft Bill.

---

[158] Ibid., 88.

[159] Bauer, Matthias, Lee-Makiyama, Hosuk, Van der Marel, Erik, and Verschelde, Bert, "The Costs of Data Localisation: Friendly Fire on Economic Recovery", ECIPE Occasional Paper, No. 3/2014. European Centre for International Political Economy (ECIPE), Brussels, 2014.

[160] Bailey, Rishab and Parsheera, Smriti, "Data Localisation in India: Questioning the Means and Ends", Working Paper No. 242. NIPFP Working Paper Series. NIPFP, 31 October 2018. https://www.ssrn.com/abstract=3356617.

### 4.4. Exemptions and exceptions for government bodies

National security and public interest are the primary drivers of data processing exemptions afforded to governments and government bodies in both India and Germany.

Article 23 of the GDPR provides an opening clause for Member States to introduce restrictions to the obligations of data controllers and to the rights of data subjects "when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society". The conditions for restrictions include the expected concerns of safeguarding "national security, defence, public security" and other concerns such as investigation and prevention of breaches and protection of the rights of data subjects. As a safeguard for preventing abuse, Article 23(2)(h) further says that Member States must provide for "the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction". The BDSG-Neu cites this Article twice in Section 32 and Section 33—both dealing with the information that a data controller must provide to a data subject. Section 34 of the BDSG-Neu reiterates the documentation requirement. It says that the "refusal to provide information shall be documented" and that the "data subject shall be informed of the reasons for refusing to provide information, unless providing the reasons in law and in fact on which the decision is based would undermine the intended purpose of refusing to provide the information". As concerns a federal public body refusing to provide information, the section mandates that in such a case "information shall be provided to the Federal Commissioner at the request of the data subject, unless the responsible supreme federal authority determines in the individual case that doing so would endanger the security of the Federation or a *Land*".

Article 9(1) of the GDPR expressly prohibits the processing of special categories of personal data, under which it counts "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation". These restrictions serve to further protect the interests and privacy of a data subject, be it from the data processing actions of a state body or a private one. However, in the very next paragraph, Article 9(2) lists out exceptions to the rule, a number of which are directly applicable to state governments. These include, among others: social security, social protection and employment; protection of vital interests of the data subject; legal proceedings; providing healthcare; archiving in public interest, historical, or statistical purposes.

With reference to the above derogations under Article 9(1), the BDSG-Neu in its Section 22 introduces exceptions to processing of "special categories of personal data" under two heads: one for both public and private bodies and another exclusively for public bodies. Exceptions under the first are limited to the purposes of healthcare and for protection of data subject rights (under social protection and social security).

Exceptions under the second head, on the other hand, are broadly under the rubric of defence and security. These include processing of said category of data when "urgently necessary for reasons of substantial public interest", "to prevent a substantial threat to public security", "necessary to prevent substantial harm to the common good or to safeguard substantial concerns of the common good", and cases where processing is "necessary for urgent reasons of defence or to fulfil supra- or intergovernmental obligations of a public body of the Federation in the field of crisis management or conflict prevention or for humanitarian measures". Added to this is the caveat that the need for such processing must outweigh the interest of the data subject.

We see national security concerns and fundamental rights posited as opposite forces rather than be posited in a framework where national security concerns work to protect the very same fundamental rights.

These themes and a similar treatment of them are seen in the Indian Draft Bill as well. What is different, however, is the way the exceptions are designed. While Germany offers a set of exceptions to an established norm when it comes to government functions and national security, the Indian Draft Bill institutes a separate norm altogether for the same. It does this with a blanket allowance for state functions, defining those as one of the many legitimate grounds for processing.

Sections 13, 14, 19, and 20 of the Indian Draft Bill fall under the chapter on legitimate "grounds for processing of personal data". Section 13 of the Bill offers a strong contrast to the provision under Section 34 of the BDSG-Neu. The German law provides for a stand-in accountability mechanism in case a government department or body refuses information to a data subject. This is in the form of the government controller being answerable to the Federal Commissioner. The Indian Bill gives the state a much broader berth. Section 13 allows for the processing of personal data when "such processing is necessary for any function of Parliament or any State Legislature" and when it is "necessary for the exercise of any function of the State authorised by law", including for the "provision of any service of benefit to the data principal from the State". The services and benefits, in the practical sense, give broad permissions to programmes like Aadhaar, where data collection, processing, and even sharing has already happened so far without a data protection statute. Section 14 of the draft Bill allows for the processing of personal data for compliance with any order of

any court or tribunal and also when "explicitly mandated under any law made by Parliament or State Legislature". Sections 19 and 20 allow the same kind of processing as under Sections 13 and 14 (state functions and legal compliance), but for sensitive personal data.

Furthermore, according to Section 42 of the Draft Bill, any data processing to achieve lawful ends of "security of state" are exempt from processing obligations that observe and protect most rights of the data principal. Sections 43 and 44 allow for exemptions from processing requirements when done for investigations and legal proceedings. They also allow for data retention after an investigation is through. The advocacy organisation Access Now has pointed out that since Indian surveillance laws are in need of reforms and an oversight mechanism—something the BN Srikrishna Committee itself has also acknowledged in its report—exemptions such as these could throw up challenges in implementing data subject rights going forward.[161]

Between the BDSG and the Indian Draft Bill, the exemptions and exceptions for the government are drafted more broadly in the latter. In the EU framework, the exemptions under Article 23(2) of the GDPR mandate that the restrictions to the rights of the data subject come with specific provisions such as the categories of personal data allowed to be processed, safeguards to prevent abuse or unlawful transfer, right of the data subject to be informed of the restrictions, and the like. In Germany in particular, a look at personal data processing by public bodies must also take into account programmes and legislations outside of the BDSG-Neu.

In what has been dubbed as the Staatstrojaner or State Trojan programme, a 2017 amendment to the German Criminal Code made room for the federal police in the country to obtain access to devices or networks via malware. The recent amendment to the Passausweisgesetz and the Passgesetz (see chapter on government IDs) also allow law enforcement to retrieve biometric photographs of those who have been issued these IDs. This kind of access has raised privacy concerns in Germany. Activists have already filed constitutional complaints against the Staatstrojaner programme. The Indian Draft Bill, however, proposes a regime where all government functions requiring processing—not just those related to security—are legitimate grounds for processing data. In this, the further discussion and input of parliamentarians before the Bill is signed into law will prove instructive.

[161] "Assessing India's Proposed Data Protection Framework: What the Srikrishna Committee Could Learn From Europe's Experience", (Access Now, 2018), https://www.accessnow.org/cms/assets/uploads/2018/09/Assessing-India%E2%80%99s-proposed-data-protection-framework-final.pdf.

### 4.5. Identifying contrasts and comparisons

In comparing the data subject rights as applied in Germany under the GDPR and as proposed by the Draft Bill in India, we see how they employ similar terminologies but differ in the application (in the case of the Draft Bill, proposed application).

A peculiar point of difference presents itself with the right to access. The Indian Draft Bill proposes a right to access a "brief summary" of personal data from the data controller. In its comments to the Indian government, the EU Commission raised this point as something that could be reconsidered to grant a data subject her data in full. However, interpretation of the right in the German jurisdiction appears to be more varied. For example, the Hessian Commissioner for Data Protection and Freedom of Information has interpreted the right to be that to a summary. Two regional courts, however, hold a different view. The right to correction in the Indian Draft Bill is framed as a right that may be exercised "where necessary" —a framing not seen in the EU context. In the right to be forgotten and the right to erasure, we see the GDPR clearly makes a reference to delinking or delisting of information that is sought to be "forgotten". A similar explicit reference is not present in the Indian Draft Bill. With the right to data portability, the two jurisdictions seem to have common ground. However, the Indian Draft Bill is clear and explicit about the categories of data that may be ported. Under the GDPR, one must depend on Recitals and Working Party 29 recommendations to interpret the same. The strongest point of difference remains with the provisions on data transfers and localisation. Both Germany and India have limited localisation requirements. The Indian Draft Bill, however, goes a step further in proposing that a copy of all sensitive personal data be stored on servers within Indian borders. The GDPR on the other hand, prescribes conditions for the transfer of EU citizens' and residents' personal data outside of the EU borders.

Exceptions for state bodies and security agencies is another point where we see the two countries converge, but only to the extent that national security can be grounds for not observing data subject rights. Under the BDSG-Neu, such exceptions come with requirements for documentation of restriction of rights. The Indian Draft Bill, on the other hand, does not propose such a documentation.

With over one year of the GDPR regime already past in the EU in general and Germany in particular, many lessons and learnings have already presented themselves. One of the first points to emerge was that the impact of the regulation extends far beyond the obviously visible objects of technology and data companies. Schools, human resource departments, and private clubs with data on their members were all to comply with the regulation. However, as it later emerged, owing to the large fines, there were cases of over-compliance, and interpretation of the law far beyond the context of activities carried out by the data control-

lers or processors. A curious example of this comes from Dormagen, a German town northwest of Cologne. In August 2018, a children's day care centre in this town distributed its usual remembrance photo album to the children at the end of the year, except it only showed the face of the child receiving the album. The faces of their friends were blackened for privacy.[162] Complexity of compliance with data requests is another issue that data controllers and processors have raised. A European software developer floated a website called shipyourenemiesgdpr.com in May 2019. Using the website, one can send a data access request to one's "enemies" (the website suggests landlords and ex-employers among other potential receivers) in order to "waste as much of their time as possible".[163] India could potentially look into investing in legal awareness to avoid results such as out-of-context compliance and the law being used as a bullying tool.

Looking at the recent and consistent statements from Indian lawmakers and business magnates, a concern most often referred to within data protection has been that of "data colonisation"—a concern that foreign control over data of Indians would replicate the conditions of the British colonial period, when a foreign power held political control over the country. Nandan Nilekani, Infosys co-founder and the chief architect of the Aadhaar programme, in August 2017 asserted the need for a policy against "data colonisation".[164] India's richest man, business magnate Mukesh Ambani—who happens to own Reliance Jio, a major telecom and internet service provider in India—also made a statement in December 2018 about "data colonisation", adding that "India's data must be controlled and owned by Indian people and not by corporates, especially global corporations".[165] In February 2019, the union minister for electronics and information technology made a similar statement, affirming the need to prevent "data imperialism".[166] India brings its own set of historically relevant anxieties to this issue, where one can observe the gradual securitisation of the subject. Under these circumstances, assertion of data subject rights in the face of the Indian government wanting to control data flows is likely to emerge as a key challenge in the coming years.

---

[162] "Datenschutz: Kita schwärzt Gesichter in Fotoalben", *Die Welt*, 2 August 2018, https://www.welt.de/vermischtes/article180429010/Datenschutz-Kita-schwaerzt-Gesichter-in-Fotoalben.html.

[163] https://shipyourenemiesgdpr.com/

[164] Pramanik, Ayan, "Need Policy against Data Colonisation: Nandan Nilekani", *Business Standard India*, 9 August 2017, https://www.business-standard.com/article/technology/need-policy-against-data-colonisation-nandan-nilekani-117080900007_1.html.

[165] PTI, "India's Data Must Be Controlled and Owned by Indians: Mukesh Ambani", *Mint,* 19 December 2018, https://www.livemint.com/Politics/nxrCcqcAFoDxyGUjZkSrNK/Indias-data-must-be-controlled-and-owned-by-Indians-Mukesh.html.

[166] ET Bureau, "Data Imperialism by Companies Not Acceptable: Ravi Shankar Prasad", *The Economic Times*, 25 February 2019, https://economictimes.indiatimes.com/news/company/corporate-trends/data-imperialism-by-companies-not-acceptable-ravi-shankar-prasad/articleshow/68146136.cms?from=mdr.

## 5. Concluding remarks

In analysing Germany's and India's responses to issues surrounding privacy and data protection, one can see a reflection of their legal, political, and economic interests, their contexts and their capabilities. Their responses and decisions not only reveal their position on privacy as a value, but they also betray the strengths and failings of their respective democratic institutions.

The two countries' outlook on these issues can be seen to be coloured by their respective political histories. Germany suffered excesses under the Nazi regime in the pre-war years, with its extensive and mechanised profiling of citizens. Later, in East Germany, the government's surveillance machinery worked to monitor citizens, intruding on their communications and daily lives to contain dissent or the possibility thereof. The country today has outlawed profiling of citizens by the government, as evidenced by the provisions in the Passgesetz and the Personalausweisgesetz. It is not just what is codified in law alone. Awareness of these historical events and times is strong in popular discourse as well. One can see this in the commentary that followed in street protests and other activism when the USA's global spying programme came to light in the summer of 2013. The immediate comparison was with East German surveillance methods, with the US National Security Agency being compared to the Stasi. Before that, in 2007, when German secretary of interior Wolfgang Schäuble proposed a longer and more extensive regime for telecommunications data retention, digital rights activists billed him "Stasi 2.0". When Germany began to trial facial recognition technologies and expand functions in video surveillance, member of the Bundestag Andrea Lindholz accused those suggesting that the state be trusted of "historical amnesia".[167]

In India, meanwhile, the anxieties of being wronged stem primarily from two and a half centuries of oppressive British colonial rule. We see this most starkly in the way the term "data colonisation" often comes up when describing the practices of foreign digital technology companies with a large user base in India. Large-scale data collection, profiling, and intrusions of privacy did not form a part of the national experience in India the way it did for Germany. However, with several international companies expanding in India, and their unhealthy data collection and processing practices being exposed in various parts of the world, India today is alive to the issues that stem from such practices. This took some evolution over time. While the government reaction to the Snowden disclosures was weak, the response to the Cambridge Analytica Scandal five years later gave the appearance of seriousness, albeit only in speech and not in action. The scandal, which unearthed the Russian

[167] "Those who suggest in principle that our state would misuse any bit of information that's available to it suffer from historical amnesia and places today's Germany on the same level as the GDR", Lindholz was reported as saying. Delcker, "Big Brother in Berlin".

interference in the US presidential elections of 2016, came to light in 2018—one year before India had its own general elections of 2019. The threat was too close and too real.

As for the state turning against the citizens with all the data it captures on them—a recognition of that can only be seen from the activist quarters, best illustrated by the legal activism against the Aadhaar programme. The state attitude here is in stark contrast with that of Germany. Privacy was not seen as an inherent value to be protected by default, but as an optional privilege easily and legitimately sacrificed at the altar of operational ease. A similar line of thought could be observed first in the arguments of those in the Constituent Assembly who argued against recognising privacy as a right, and then later in the arguments of the proponents of the Aadhaar programme, who dismissed concerns about privacy as elitist ideas unmindful of the ground realities of the underprivileged.

These ideas find an echo in the design and use of biometric ID systems in both the countries. The Personalausweisgesetz says that the number assigned to the ID document (the Ausweis) may not be linked to the identity of the ID holder. This is in complete contrast to India, where the Aadhaar number is treated as an identity number that must be cited to receive welfare benefits from the state. In fact, in the 2019–20 annual budget, the central government even announced that one can cite their Aadhaar number instead of their Permanent Account Number (PAN) while filing taxes.[168] Germany, as mentioned above, specifically outlaws the creation of a national ID database. Aadhaar, on the other hand, functions with a Central Identities Repository, or CIDR. However, the German protection against the creation of an ID repository stands threatened after a 2017 amendment to the Passgesetz and the Passausweisgesetz. Law enforcement agencies now have access to a database of passport photos, and the means to automatically retrieve them, letting them create a potential database of biometric photos of all citizens.

When it comes to authentication functions using identity instruments, both Germany and India offer an option for the same to ID holders. However, the scale and design of such operations differ significantly. India went through a period of mandatory linking of Aadhaar to mobile phone connections, bank accounts, and the like. While linking to private operations today is a possible option, it remains mandatory for receiving welfare benefits and for filing tax returns. In Germany, there is a clear attempt (although an unsuccessful one, judging by the numbers) at nudging people towards using electronic IDs for online transactions and for e-governance functions. While there are no strict rules mandating the same, the pushback against it remains strong. This illustrates a key difference between state-citizen

[168] "Explainer: Can You Now Use Aadhaar in Place of a PAN Card?" *Scroll.in*, 9 July 2019, https://scroll.in/article/929839/explainer-can-you-now-use-aadhaar-in-place-of-a-pan-card.

relationships in the two countries. The Indian state takes on the role of a provider controlling access in exchange for data, positioning itself in a place of relatively more power against the dependent citizen. The German state, on the other hand, is seen to be using tactics of persuasion with the balance of power still in the citizens' hands when it comes to deciding to use the electronic IDs for verification, even with the function switched on by default.

While we see function creep in action in both the countries, in Germany, it can be observed along with securitisation of the ID infrastructure. The decision of the constitutional court in the pending complaint against automated retrieval of biometric ID photos would clarify the legal principles in this case.

On the count of surveillance, the two countries differ starkly. India offers little information on its chief intelligence agencies—even their charters are not publicly known. No intelligence operation has yet been declassified. The agencies also do not come under any parliamentary or judicial oversight. Germany, on the other hand, offers information about the charters and duties of its agencies and subjects them to parliamentary and judicial oversight. The presence of these mechanisms, however, has not prevented procedural lapses. We saw that with the German intelligence sharing with the US, which slipped through the oversight cracks. Discovered thanks to the Snowden revelations, these transgressions saw tangible action in the form of parliamentary inquiries, investigations, and a reform of the oversight mechanism. The reforms to oversight, introduced in 2017, create additional oversight bodies and also open the agencies up to additional scrutiny, for example, from the office of the Federal Data Protection Commissioner. However, these changes have been criticised for not going far enough, and in fact, for legalising data sharing operations. India, on the other hand, has seen support from senior public figures for introducing parliamentary and judicial oversight. However, there have been no serious or definitive efforts in that direction. A public interest litigation in India asking for intelligence agencies to be brought under financial audit was rejected by the Supreme Court on security grounds. The argument for security has significant currency in a country like India, which has gone to war with two neighbours—Pakistan and China—and continues to have strained relations with them. This not only makes securitisation of issues wide-ranging but also gives it acceptability and popular appeal.

Another strong point of contrast between India and Germany emerges on the count of legal frameworks around privacy and data protection. Germany has close to five decades of experience in enacting, revising, and evolving data protection statutes. Secrecy of correspondence and inviolability of living quarters was encoded into the Basic Law. India, on the other hand, acknowledged privacy to be a fundamental right only in 2017. A Draft Personal Data

Protection Bill, released to the public in the summer of 2018, has been hanging fire for more than a year. Though on the surface, the Draft Personal Data Protection Bill, 2018 appears to follow the format of the EU-wide General Data Protection Regulation, it gives states significantly more power through broad exemptions for "security of state" and for legal proceedings. The Draft Bill misses the chance to create an oversight mechanism for security agencies, giving them blanket permissions to collect and process data instead. User rights, which were the focus of this report when analysing legal frameworks, are also qualified in the proposed Indian Draft Bill. In the Indian context, we see securitisation of the proposed data transfer mechanisms as well, with the government advocating for localisation. Sluggish mutual legal assistance treaty processes (MLATs) provide the animus for this proposal. While the German adaptation of the GDPR appears to be aimed at giving the individual more control over their data, the Draft Bill in India appears to place the control in the hands of the Indian state.

Going by the events of the past decade, claims to democracy will continue to be tested on the standards of protecting privacy. While both the countries have taken steps towards updating the laws, they are also heavily investing in developing technologies like facial recognition and artificial intelligence for state functions, especially in crime prevention. While legal and regulatory limits might be in for a pressure test with these developments, it is accountability and oversight structures that will need to be watertight to contain excesses and evade abuses. The principles behind the application of technologies, development of law, and establishment of accountability and oversight measures will reveal the directions the countries want to take as functioning democracies.

## Bibliography


Access Now. "Assessing India's Proposed Data Protection Framework: What the Srikrishna Committee Could Learn from Europe's Experience". https://www.accessnow.org/cms/assets/uploads/2018/09/Assessing-India%E2%80%99s-proposed-data-protection-framework-final.pdf.

Acharya, Bhairav. "Comments on the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011". Centre for Internet and Society, 31 March 2013. https://cis-india.org/internet-governance/blog/comments-on-the-it-reasonable-security-practices-and-procedures-and-sensitive-personal-data-or-information-rules-2011.

Agarwal, Vibhuti. "Q&A: NATGRID Chief Raghu Raman". *WSJ* (blog), 29 June 2011. https://blogs.wsj.com/indiarealtime/2011/06/29/qa-natgrid-chief-raghu-raman/.

Arun, Chinmayi. "Paper-Thin Safeguards and Mass Surveillance in India". *National Law School of India Review*, no. 26 (2014).

Bailey, Rishab, and Parsheera, Smriti. "Data Localisation in India: Questioning the Means and Ends". Working Paper No. 242. NIPFP Working Paper Series. NIPFP, 31 October 2018. https://www.ssrn.com/abstract=3356617.

Banisar, David. "National Comprehensive Data Protection/Privacy Laws and Bills 2019". ARTICLE 19: Global Campaign for Free Expression, 1 August 2019. http://dx.doi.org/10.2139/ssrn.1951416.

Bauer, Matthias, Lee-Makiyama, Hosuk, Van der Marel, Erik, and Verschelde, Bert. "The Costs of Data Localisation: Friendly Fire on Economic Recovery". ECIPE Occasional Paper, No. 3/2014. European Centre for International Political Economy (ECIPE), Brussels, 2014.

Bhandari, Vrinda, Parsheera, Smriti, and Rahman, Faiza. "India's Communication Surveillance through the Puttaswamy Lens". *The Leap Blog* (blog), 18 May 2018. https://blog.theleapjournal.org/2018/05/indias-communication-surveillance.html.

Bhatia, Rahul. "Exclusive: Police Detain Man in Probe of Alleged Data Leak at India's Jio". *Reuters*, 11 July 2017. https://www.reuters.com/article/us-reliance-jio-cyber-exclusive-idUSKBN19W1E0.

Black, Edwin. *IBM and the Holocaust: The Strategic Alliance Between Nazi Germany and America's Most Powerful Corporation*. Little, Brown & Company, 2001.

Chaturvedi, Aditi. "GDPR and India". Center for Internet and Society, 17 October 2017. https://cis-india.org/internet-governance/files/gdpr-and-india.

Chee, Foo Yun. "You Have the Right to Be Forgotten by Google - but Only in Europe". *Reuters*, 24 September 2019. https://www.reuters.com/article/us-eu-alphabet-privacy-idUSKBN1W90R5.

Choudhary, Amit Anand. "No Fundamental Right to Privacy to Citizens: Centre Tells SC". *The Times of India*, 22 July 2015. https://timesofindia.indiatimes.com/india/No-fundamental-right-to-privacy-to-citizens-Centre-tells-SC/articleshow/48171323.cms

Cronin, David. "Biometrics – a Passport to Security?". Politico, 22 June 2005. https://www.politico.eu/article/biometrics-a-passport-to-security/.

Dachwitz, Ingo. "Im Gesetz zum elektronischen Personalausweis versteckt sich ein automatisierter Abruf für Geheimdienste [Update]". *netzpolitik.org*, 24 April 2017. https://netzpolitik.org/2017/im-gesetz-zum-elektronischen-personalausweis-versteckt-sich-ein-automatisierter-abruf-fuer-geheimdienste/.

Datta, Saikat. "Never Mind the 'Snooping' on Rahul, the Government Is Watching over Even Your Internet Usage". *Scroll.in*, 16 March 2015. https://scroll.in/article/713966/never-mind-the-snooping-on-rahul-the-government-is-watching-over-even-your-internet-usage.

De Hert, Paul, Papakonstantinou, Vagelis, Malgieri, Gianclaudio, Beslay, Laurent, and Sanchez, Ignacio. "The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services". *Computer Law & Security Review* 34, no. 2 (April 2018), https://doi.org/10.1016/j.clsr.2017.10.003.

Deutsche Welle. "Germany Introduces Biometric Passports". 1 November 2005. https://www.dw.com/en/germany-introduces-biometric-passports/a-1762338.

Die Welt. "Datenschutz: Kita schwärzt Gesichter in Fotoalben". 2 August 2018. https://www.welt.de/vermischtes/article180429010/Datenschutz-Kita-schwaerzt-Gesichter-in-Fotoalben.html.

Drèze, Jean and Khera, Reetika. "Aadhaar's $11-Billion Question". *The Economic Times Blogs* (blog), 7 February 2018. https://economictimes.indiatimes.com/blogs/et-commentary/aadhaars-11-bn-question/.

Dutta, Prabhash K. "Right to Privacy: 5 Bills yet No Law, How Parliament Has Dealt with Personal Data Protection". *India Today*, 24 August 2017. https://www.indiatoday.in/india/story/right-to-privacy-fundamental-right-parliament-1031136-2017-08-24.

Elteste, Ulrike, Van Quathem, Kristof, and Oberschelp de Meneses, Anna. "German Supervisory Authorities Issue Guidance on Data Subject Rights". *Inside Privacy*, 12 July 2019. https://www.insideprivacy.com/international/european-union/german-supervisory-authorities-issue-guidance-on-data-subject-rights/.

ET Bureau. “Data Imperialism by Companies Not Acceptable: Ravi Shankar Prasad”. *The Economic Times*, 25 February 2019. https://economictimes.indiatimes.com/news/company/corporate-trends/data-imperialism-by-companies-not-acceptable-ravi-shankar-prasad/articleshow/68146136.cms?from=mdr.

Freude, Alvar and Freude, Trixy. “Echoes of History: Understanding German Data Protection”. Bertelsmann Foundation, 1 October 2016. https://www.bfna.org/research/echos-of-history-understanding-german-data-protection/.

Gärditz, Klaus. “Legal Restraints on the Extraterritorial Activities of Germany’s Intelligence Services”. In *Privacy and Power*, ed. Russell A. Miller (Cambridge: Cambridge University Press, 2017), https://doi.org/10.1017/CBO9781316658888.016.

Gesellschaft für Freiheitsrechte. “Automatisierte Passbildabfrage”. 6 December 2018. https://freiheitsrechte.org/automatisierte-passbildabfrage/.

Gesley, Jenny. “Foreign Intelligence Gathering Laws: Germany”. Library of Congress web page, June 2016. https://www.loc.gov/law/help/intelligence-activities/germany.php.

Goschler, Constantin and Wala, Michael. “Die Geheimnisse eines Geheimdienstes”. *Rubin Wissenschaftsmagazin*. Spring 2014. https://www.ruhr-uni-bochum.de/geschichte-bfv/pdf/2014_rubin_verfassungsschutz.pdf.

Gupta, Apar and Uppaluri, Ujwala. “A Fundamental Error”. *The Hindu*, 1 August 2018. https://www.thehindu.com/opinion/lead/a-fundamental-error/article24566374.ece.

Gupta, Shekhar. “God, Please Save India from Our Upper Class Aadhaarophobics”. *The Print* (blog), 25 September 2018. https://theprint.in/opinion/save-india-wine-n-cheese-aadhaarophobics/27456/.

Hannah, Matthew G. *Dark Territory in the Information Age: Learning from the West German Census Controversies of the 1980s* (Burlington, Vt: Ashgate, 2010).

Hornung, Gerrit and Schnabel, Christoph. “Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination”. *Computer Law & Security Review* 25, no. 1 (January 2009). https://doi.org/10.1016/j.clsr.2008.11.002.

Hornung, Gerrit and Schnabel, Christoph. “Data Protection in Germany II: Recent Decisions on Online-Searching of Computers, Automatic Number Plate Recognition and Data Retention.” *Computer Law & Security Review* 25, no. 2 (January 2009). https://doi.org/10.1016/j.clsr.2009.02.008.

India Today. “Sharing Aadhaar Details Safe or Not Safe? UIDAI Can’t Make up Its Mind and Clear Confusion”. 12 March 2018. https://www.indiatoday.in/technology/news/story/sharing-aadhaar-details-safe-or-not-safe-uidai-can-t-make-up-its-mind-and-clear-confusion-1187506-2018-03-12.

Inside Privacy. “German Court Decides on the Scope of GDPR Right of Access”. 8 August 2019. https://www.insideprivacy.com/international/european-union/german-court-decides-on-the-scope-of-gdpr-right-of-access/.

Joseph, Manu. “When You Give Your Biometrics to Modi”. https://www.livemint.com, 7 April 2017. https://www.livemint.com/Leisure/28JmBgGLgWLclLxQtzd9KI/When-you-give-your-biometrics-to-Modi.html.

Kambampati, Sushil. “Aadhaar: The Indian Biometric ID System Has Potential but Presents Many Concerns”. *Heinrich Böll Stiftung, 14* February 2018. https://www.boell.de/en/2018/02/07/aadhaar-indian-biometric-id-system-has-potential-presents-many-concerns.

Khaira, Rachna. “Rs 500, 10 Minutes, and You Have Access to Billion Aadhaar Details”. *The Tribune*, 4 January 2018. https://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html.

Kochanek, Stanley A. and Hardgrave, Robert L. *India: Government and Politics in a Developing Nation* (Boston: Thomson Wadsworth, 2000).

Krieger, Wolfgang. “US Patronage of German Postwar Intelligence”. In *Handbook of Intelligence Studies*, edited by Loch K. Johnson, 1st ed. Routledge, 2007, https://doi.org/10.4324/9780203089323.

Matthan, Rahul. *Privacy 3.0*, 2018th ed. (HarperCollins Publishers India).

Miller, Russell A. “Intelligence Oversight -- Made in Germany”. In *Global Intelligence Oversight: Governing Security in the Twenty-First Century*, edited by Zachary K. Goldman and Samuel James Rascoff. New York, NY, Oxford University Press, 2016.

Moneylife. “Nandan Nilekani Is Part of Every Committee and Group That Is Making Aadhaar Mandatory”. 1 October 2013. http://www.moneylife.in/article/nandan-nilekani-is-part-of-every-committee-and-group-that-is-making-aadhaar-mandatory/34677.html.

Müller, Volker. “Deutscher Bundestag - Arne Schlatmann zum Bevollmächtigten des Kontrollgremiums ernannt”. Deutscher Bundestag, 10 January 2017. https://www.bundestag.de/dokumente/textarchiv/2017/kw02-schlatmann-pkgr-487768.

NDTV. “Supreme Court Junks Plea Seeking To Make Intelligence Agencies Accountable”. 23 February 2016. https://www.ndtv.com/india-news/supreme-court-junks-plea-seeking-to-make-intelligence-agencies-accountable-1280316.

Noack, Torsten and Kubicek, Herbert. “The Introduction of Online Authentication as Part of the New Electronic National Identity Card in Germany”. *Identity in the Information Society* 3, no. 1 (1 July 2010): 95, https://doi.org/10.1007/s12394-010-0051-1.

NOYB. “CJEU Hears Case on EU-US Data Transfers (Standard Contractual Clauses and Privacy Shield)”. Accessed 19 August 2019. https://noyb.eu/cjeu-case/, https://noyb.eu/cjeu-case/.

Otwinowski, Martha. “Tailor-Made Laws: The State of Surveillance in Germany”. *Index on Censorship*, 7 November 2016. https://www.indexoncensorship.org/2016/11/tailor-made-laws-the-state-of-surveillance-in-germany/.

Parker, Ian. “The I.D. Man”. *The New Yorker*, 26 September 2011. https://www.newyorker.com/magazine/2011/10/03/the-i-d-man.

Pohle, Julia, Hösl, Maximilian, and Kniep, Ronja. “Analysing Internet Policy as a Field of Struggle”. *Internet Policy Review* 5, no. 3 (25 July 2016). https://policyreview.info/articles/analysis/analysing-internet-policy-field-struggle.

Pramanik, Ayan. “Need Policy against Data Colonisation: Nandan Nilekani”. *Business Standard India*, 9 August 2017. https://www.business-standard.com/article/technology/need-policy-against-data-colonisation-nandan-nilekani-117080900007_1.html.

PTI. “India’s Data Must Be Controlled and Owned by Indians: Mukesh Ambani”. *Mint*, 19 December 2018. https://www.livemint.com/Politics/nxrCcqcAFoDxyGUjZkSrNK/Indias-data-must-be-controlled-and-owned-by-Indians-Mukesh.html.

Pütter, Norbet. “Germany The Federal Republic’s Security Services from the Cold War to the ‘New Security Architecture’”. *Statewatch Journal* 19, no. 4 (December 2009).

Rajagopal, Krishnadas. “Major Arguments in the Right to Privacy Case” *The Hindu*. 24 August 2017. https://www.thehindu.com/news/national/major-arguments-in-the-right-to-privacy-case/article19551038.ece.

Raghavan, Srinath. “After 50 Years of RAW, There Are Still No Declassified Documents or an Official History”. *ThePrint* (blog), 18 September 2018. https://theprint.in/opinion/why-was-raw-formed-and-what-has-india-learnt-after-50-years-of-its-existence/119811/.

Raman, B. *The Kaoboys of R&AW: Down Memory Lane*, 2013 US edition (Lancer Publishers, 2007).

Raman, B. "Making Intelligence Agencies Accountable". *Outlook Magazine*, 20 January 2010. https://www.outlookindia.com/website/story/making-intelligence-agencies-accountable/263866.

Ramanathan, Usha and Ray, Subhadeepta. "A Curious State of Affairs". *Seminar*, no. 641, India 2012 (2013). http://www.india-seminar.com/2013/641/641_usha_ramanathan_et_al.htm.

Rani, Sarita. "Snooping: The IB's Mandate Has Always Been to Protect India's Rulers from Indians." *The Wire*. Accessed 25 December 2018. https://thewire.in/government/snooping-the-ibs-mandate-has-always-been-to-protect-indias-rulers-from-indians.

Rao, YS. "The Mysterious Case of CBI's Legality". *Governance Now*, 3 June 2019. https://www.governancenow.com/news/regular-story/the-mysterious-case-of-cbis-legality.

Rath, Christian. "Zugriff auf Passfotos aller Bundesbürger: Fotoalben für Geheimdienste". *Die Tageszeitung: taz*, 26 April 2017, sec. Politik. https://taz.de/!5404643/.

Saikia, Nandita. "On The Indian Government's Clarification On IT Rules And Personal Data". *MediaNama* (blog), 26 August 2011. https://www.medianama.com/2011/08/223-on-the-indian-governments-clarification-on-it-rules-and-personal-data/.

Schneier, Bruce. "Security and Function Creep". *IEEE Security Privacy* 8, no. 1 (January 2010) https://doi.org/10.1109/MSP.2010.47.

Schwartz, Paul M and Peifer, Karl-Nikolaus. "Prosser's Privacy and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Concept". *California Law Review* 98, 2010.

Scroll Staff. "Explainer: Can You Now Use Aadhaar in Place of a PAN Card?" *Scroll.in*, 9 July 2019. https://scroll.in/article/929839/explainer-can-you-now-use-aadhaar-in-place-of-a-pan-card.

Shaffer, Ryan. "Unraveling India's Foreign Intelligence: The Origins and Evolution of the Research and Analysis Wing". *International Journal of Intelligence and CounterIntelligence* 28, no. 2 (3 April 2015): 260. https://doi.org/10.1080/08850607.2015.992754.

Sinha, Amber and Kodali, Srinivas. "Information Security Practices of Aadhaar (or Lack Thereof): A Documentation of Public Availability of Aadhaar Numbers with Sensitive Personal Financial Information". 16 May 2017.

Sloot, Bart van der. "Do Data Protection Rules Protect the Individual and Should They? An Assessment of the Proposed General Data Protection Regulation". *International Data Privacy Law* 4, no. 4 (1 November 2014). https://doi.org/10.1093/idpl/ipu014.

Spiegel Online. "Neues Personalausweis-Gesetz: Bundestag erlaubt massenhaften Zugriff auf Passfotos". 19 May 2017. https://www.spiegel.de/netzwelt/netzpolitik/elektronischer-personalausweis-eid-bundestag-erlaubt-zugriff-auf-ausweis-fotos-a-1148394.html.

Spitz, Malte. "Germans Loved Obama. Now We Don't Trust Him". *The New York Times*, 19 October 2018. https://www.nytimes.com/2013/06/30/opinion/sunday/germans-loved-obama-now-we-dont-trust-him.html.

Sreevatsan, Ajai. "'We Have to Factor in Data Privacy in Census Design and Methodology'". *Mint*, 22 January 2018. https://www.livemint.com/Politics/04X1G5qikIWynGdtIxyAuO/We-have-to-factor-in-data-privacy-in-census-design-and-meth.html.

Subramanian, K S. "'National Security' for Whom?" *Economic and Political Weekly* 49, no. 25 (21 June 2014).

The Economic Times. "Aadhaar Will Identify Genuine Beneficiaries of Schemes: Centre to SC." 21 March 2018. https://economictimes.indiatimes.com/articleshow/63402494.cms?from=mdr&utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst.

The Hindu. "Biometric Data in State Hubs Destroyed: UIDAI". 22 February 2018. https://www.thehindu.com/news/national/biometric-data-in-state-hubs-destroyed-uidai/article22827716.ece.

The Hindu. "UIDAI Introduces Two-Tier Security to Shield Aadhaar Data". 10 January 2018. https://www.thehindu.com/news/national/uidai-introduces-virtual-id-to-address-privacy-concerns/article22411683.ece.

The Hindu Business Line. "National Tech Research Body to Be Housed in Hyderabad". 25 February 2010. https://www.thehindubusinessline.com/todays-paper/tp-economy/National-tech-research-body-to-be-housed-in-Hyderabad/article20163734.ece.

The Times of India. "Explain Intelligence Bureau's Legality, HC Tells Centre". 26 March 2012. https://timesofindia.indiatimes.com/india/Explain-Intelligence-Bureaus-legality-HC-tells-Centre/articleshow/12408605.cms.

The Times of India. "Finally, Govt Clears Central Terror Agency, Tougher Laws". 16 December 2008. https://timesofindia.indiatimes.com/india/Finally-govt-clears-central-terror-agency-tougher-laws/articleshow/3842368.cms.

The Times of India. “Foreign-Funded NGOs Stalling Development: IB Report”. 12 June 2014. https://timesofindia.indiatimes.com/india/Foreign-funded-NGOs-stalling-development-IB-report/articleshow/36411169.cms.

Traynor, Ian, Oltermann, Philip, and Lewis, Paul. “Angela Merkel’s Call to Obama: Are You Bugging My Mobile Phone?” *The Guardian*, 24 October 2013. https://www.theguardian.com/world/2013/oct/23/us-monitored-angela-merkel-german.

Vaughn, Bruce. “The Use and Abuse of Intelligence Services in India”. *Intelligence and National Security* 8, no. 1 (January 1993). https://doi.org/10.1080/02684529308432188.

Wæver, Ole. “Securitisation and Desecuritisation”. In *On Security*, ed. Ronnie D. Lipchutz, 1995, https://www.libraryofsocialscience.com/assets/pdf/Waever-Securitization.pdf.

Wetzling, Thorsten. “Germany’s Intelligence Reform: More Surveillance, Modest Restraints and Inefficient Controls”. June 2017. https://www.stiftung-nv.de/sites/default/files/snv_thorsten_wetzling_germanys_foreign_intelligence_reform.pdf.

World Bank Group. “World Development Report 2016: Digital Dividends”. 17 May 2016. https://www.worldbank.org/en/publication/wdr2016.

Xynou, Maria. “India’s Central Monitoring System (CMS): Something to Worry About?” The Centre for Internet and Society. 30 January 2014. https://cis-india.org/internet-governance/blog/india-central-monitoring-system-something-to-worry-about.