

JUDICIAL DATA REGULATION

DISCUSSION PAPER II

Regulatory
Framework For Data
Protection And
Open Courts

JULY 2021





ACKNOWLEDGEMENTS

This paper is an independent,
non-commissioned piece of academic work,
authored by Aakanksha Mishra and Siddharth
Mandrekar Rao.

The authors would like to sincerely thank
Surya Prakash B.S. and Leah Verghese for
their able guidance throughout the research
work and for reviewing the paper.

The authors are grateful for the valuable
suggestions of Harish Narasappa, Prashant
Reddy, Smriti Parsheera, Shweta Mohandas
and Malavika Raghavan. Lastly, the authors
would also like to acknowledge the efforts of
Sandhya P.R. and Shruthi Naik at DAKSH in
reviewing and editing the paper.

CONTENTS

1	INTRODUCTION
2	CORE VALUES OF A JUDICIAL SYSTEM
5	PROPOSED DATA REGULATIONS AND WHY A NEW SCHEME IS NECESSARY
12	HOW SHOULD JUDICIAL DATA BE REGULATED?
42	ANNEXURE 1
46	ANNEXURE 2
49	ANNEXURE 3

INTRODUCTION

This paper is the second in the series of Discussion Papers on Judicial Data Regulation. The first paper¹ (henceforth 'Paper I') discusses how the Indian judiciary traditionally balanced the principle of open courts with the right to privacy and highlights the concerns around judicial data in the electronic age. This paper proposes a framework for the regulation of judicial data and access to court records. The approach in this framework furthers the goals of open justice and transparency, while addressing the concerns of privacy that the digital environment has given rise to. Privacy issues are heightened in the digitisation age due to the loss of practical obscurity that was available in the paper-based judicial system. The proposed framework and solutions are framed in the context the progress in digitalisation made by the Indian judiciary thus far and will take into consideration the challenges that may arise from such technological upgradation in the future. In doing so, we illustrate how conventional approaches to data protection are inadequate for judicial data.

Chapter II establishes that as a starting point, the development of information systems within the judiciary must be based on a sound understanding of the distinctive requirements and expectations of a judicial system, and the principle of open courts. In Chapter III, we discuss the application of the two recently proposed data protection frameworks, the Personal Data Protection Bill, 2019 (PDP Bill) and the Draft Report by the Committee of Experts on Non-Personal Data Governance Framework, in the judicial sector. In doing so, we aim to illustrate how conventional approaches to data protection are inadequate for judicial data. Chapter IV provides detailed recommendations on how judicial data should be regulated, encompassing classes of data, roles in relation to it, means of regulation, rights and responsibilities in relation to the data and a roadmap towards arriving at a regulatory framework.

¹ DAKSH. 2021. Paper I: Balancing Open Courts with the Right to Privacy – The Indian Perspective

CORE VALUES OF A JUDICIAL SYSTEM

Digital processes have a powerful role to play in the modernisation of justice systems. They have the potential to transform the functioning of organisations, increasing efficiency and effectiveness. This can be done through redesigning of processes and a significant commitment to exploiting the potential of electronically stored data, to provide faster and better information to manage the dispensation of justice. However, technological advancements are not an end in themselves. We should be weary of unquestioningly adopting technologies into the judicial sector without accounting for its particular requirements, conditions, and core values². The objective of recent efforts to modernise court information systems is typically to facilitate the interoperability and information exchange to increase efficiency. The design of information systems and the policies that govern management of court information must preserve the independence of the judiciary and principles of open justice. Therefore, we must explore the emerging possibilities that new technologies afford for better serving user requirements, promoting public confidence, and ensuring an appropriate balance between open justice and other countervailing interests.

In many jurisdictions, it is increasingly necessary to find effective new ways to implement control over electronic court records to establish the same controls that were available when they were maintained on paper. This entails a shift of focus away from physicality and presence towards the development of policies that not only guide operational practice but can also be implemented within and enforced by the technology architecture that underpins our court systems. This requires a clear and conscious articulation of judicial values and a widespread awareness of the unique characteristics of courts. Those involved in designing court information management systems, and formulating policies need to fully appreciate the values that are unique to the court environment, such as judicial independence and open courts to avoid costly mistakes from misunderstanding or incorrect assumptions³.



² 'Recommendation Rec(2001) 2 of the Committee of Ministers to member states concerning the design and re-design of court systems and legal information systems in a cost-effective manner', Council of Europe, 28 February 2001

³ Jo Sherman. 2013. 'Court Information Management – Policy Framework to Accommodate the Digital environment', Canadian Judicial Council, available online at: <https://cjc-ccm.ca/sites/default/files/documents/2019/Policy%20Framework%20to%20Accommodate%20the%20Digital%20Environment%202013-03.pdf> (last accessed on 14 June 2021).

In the context of designing policies governing access to judicial records, open justice is the primary guiding principle. There is no unitary concept or definition of open justice. In fact, open justice is better viewed as a set of principles that mediate between courts and the public. It is underpinned by broader values of safeguarding public access to information about courts and their activities. Further, it facilitates other democratic values – the right to know the law and to understand its application, permitting citizens to observe and evaluate the operation of government, and a repugnance for arbitrary power. Understanding the multiple facets of open justice can have important ramifications for the manner in which open justice will be upheld by courts tasked with balancing competing values⁴.

The public interest in obtaining access to detailed and knowledgeable information about court processes should never be curtailed without establishing justifiable and legitimate reasons to do so. In the absence of detailed and accurate information, misconception and prejudice is likely to flourish. The need to ensure good information is particularly acute in cases which depend on a detailed documentary record, or which turn on technical arguments. Although there are risks inherent in openness, retreating to covertness holds tremendous dangers for the justice system and for democratic governance⁵.

The current position of access to court records in India can be generalised as follows:

1. Public (non-parties) do not have an automatic right to access documents to court records, except where and to the extent that legislation or the rules of court confer such a right.
2. The rules of the court form the primary repository of rules governing availability of documents to the public (non-parties).
3. Where leave is required to access such documents, the court or the registrar exercises discretion in balancing countervailing considerations such as confidentiality, privacy, and right to fair trial. The principle of open justice is central to the court's consideration.

In Paper I, we discussed at length how technology has enabled easier, improved, and widespread access to judicial information. In doing so, technology has degraded the level of “practical obscurity” that was available in case of paper-based court records. Practical obscurity refers to the creation of practical barriers which make it difficult to gain access to court records even when there is no legal obstacle, such as restriction on time of access, need to travel physically to the files location etc . Therefore, a court record access policy in the digital age must aim to preserve the protections afforded by practical obscurity without impairing the court's openness.

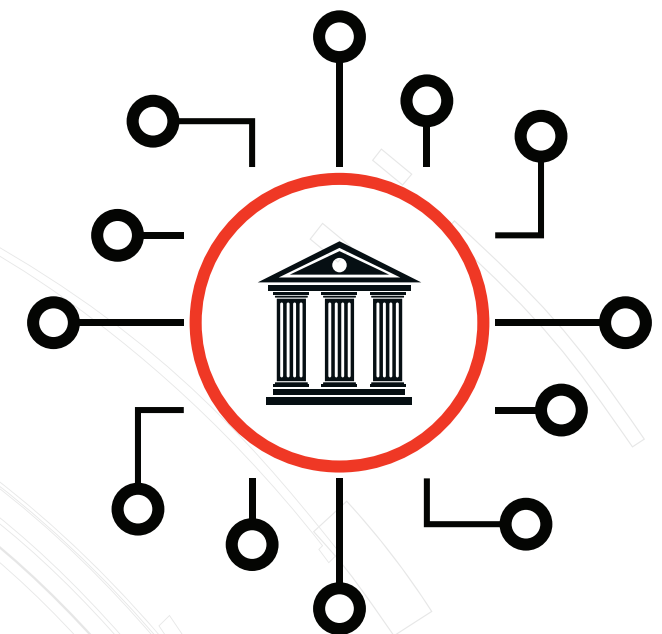
⁴ Cunliffe Emma. 2012. 'Open Justice: Concepts and Judicial Approaches', Federal Law Review, 40: 385-411

⁵ Cunliffe Emma. 2012. 'Open Justice: Concepts and Judicial Approaches', Federal Law Review, 40: 385-411

Open justice must not be equated with unfettered access to all court records. The competing considerations underlying any access regime should be balanced by identifying a set of documents which are ordinarily treated in a manner consistent with free access and subjecting all other documents to an additional level of scrutiny before making them available to non-parties. The first category should include documents which are open to public access without requiring the court's permission. This should contain documents essential to the administration of justice to which public access should be uninhibited. These would include documents that form the core of every judicial decision, i.e., documents which inform the court what the dispute is, what each party has to say in respect of their position and how the court adjudicates the dispute⁶. At present, this includes judgements and orders given or made in public, and access to live courtroom proceedings. In addition, the judiciary must look at the feasibility of making other categories of documents, such as pleadings and transcriptions, open to public in the future. This requires changes in legislation and court rules which must be undertaken in a consultative manner. Moreover, the timing of access to such documents will also have to be considered. For example, since pleadings contain contested information, it should be disclosed to the public only after the conclusion of the case to preserve the integrity of the judicial process. Notwithstanding this, the documents in the first category may sometimes contain information which should not be released for public consumption. Therefore, the court should retain the power to restrict access or impose conditions on the use of the information accessed, either on application of a party or of its own motion,

only to the extent necessary in a given circumstance. Furthermore, the onus should not be on the court to trawl through the documents in search of information that should not be disclosed. Instead, the onus should be on the parties and their lawyers to draw the court's attention to such information through an application. The second category will contain all the residual documents that do not fall in the first category and the unavailability of which will not substantially impair the ability to understand the judicial decision in a given case. This will include judgments or orders given in-camera or restricted from being reported pursuant to a court order or statute, affidavits, exhibits, material submitted as evidence etc. Access to this category of documents will require the court's permission and a demonstration of sufficient and legitimate interest in the case concerned⁷.

Thus, threats to open justice are best managed by an analytical framework which systematically identifies both the benefits of open justice and the countervailing values that are at stake in a given case, and which seeks to provide maximum protection to all of these values in a principled manner.



⁶ Vanessa Yeo. 2011. 'Access To Court Records: The Secret to Open Justice', Singapore Journal of Legal Studies, 510–532.

⁷ Vanessa Yeo. 2011. 'Access To Court Records: The Secret to Open Justice', Singapore Journal of Legal Studies, 510–532.

PROPOSED DATA REGULATIONS AND WHY A NEW SCHEME IS NECESSARY

Recent developments in data regulation in India have not yet led to concrete policy or accounted for the demands, concerns, and contextual considerations specific to judicial records.

The Personal Data Protection Bill, 2019 (PDP Bill) currently pending before a Joint Parliamentary Committee⁸ is loosely based on a bill drafted by the Justice Srikrishna Committee⁹, which was formed to develop a personal data protection framework for India. The PDP Bill applies to personal data created, collected, stored, or used in India¹⁰. It regulates the processing of personal data by people, companies, and the State¹¹. However, Clause 36(c) specifically exempts courts and tribunals in India from significant parts of the Bill if they process data in the exercise of any judicial function. Courts and tribunals are exempted from most of the substantive provisions of the Bill, in

order to ensure independence in the performance of their judicial functions.

In September 2019, the Ministry of Electronics and Information Technology (MEITY) constituted a committee to propose a framework for the regulation of Non-Personal Data (NPD), which is defined as data other than those which would be classified as personal data in the PDP Bill¹³. The Committee submitted its report in July 2020¹⁴ and released a revised report in December 2020¹⁵. The NPD framework, aims to harness economic value of non-personal data by making it available to private players for commercial use in order to foster innovation and competition¹⁶.

The PDP Bill and the NPD Report suffer from deficiencies, inconsistencies, and gaps that would make them unsuitable for judicial data. The categories

⁸ Lok Sabha. 2020. 'Joint Committee on the Personal Data Protection Bill, 2019', Lok Sabha, available online at http://loksabha.nic.in/Committee/CommitteeInformation.aspx?comm_code=73&tab=1 (accessed on 3 October 2020)

⁹ Committee of Experts under the Chairmanship of Justice B.N. Srikrishna. 2018. 'A Free and Fair Digital Economy Protecting Privacy, Empowering Indians', Ministry of electronics and Information Technology, 27 July, available online at https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf (accessed on 29 December 2020)

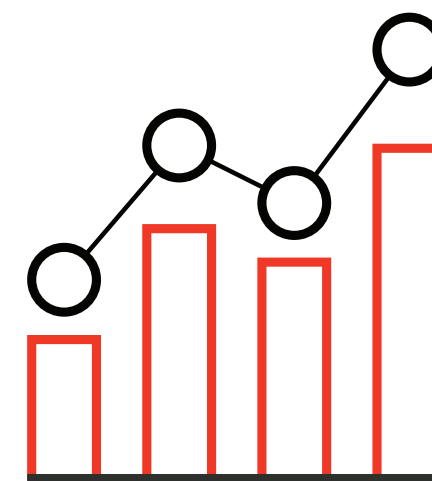
¹⁰ Clause 2, PDP Bill, 2019

¹¹ Clause 2, PDP Bill, 2019

¹² Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, 'A Free and Fair Digital Economy Protecting Privacy, Empowering Indians'

of data described in these proposed frameworks are not directly connected to the level of harm that can be inflicted upon the person that the data pertains to, through the use of that data. They are too coarse to be used in determining the sensitivity of data fields and their relevance and role in the process of judicial decision making, making them inappropriate for regulation of judicial data. The roles set out in these frameworks and the associated rights and obligations may not be appropriate for the roles and processes in which data is used by participants in the judicial process, including lawyers and litigants, judges, court staff, the police and other investigation agencies, public prosecutors, and prison authorities. The NPD framework has not accounted for judicial independence in the way the PDP Bill has. In many circumstances, the application of provisions of these frameworks clash with open justice, as will be discussed below. The NPD framework has not accounted for judicial independence in a similar manner to the PDP Bill. Therefore, the judiciary needs its own policies with regard to data protection and disclosure to protect open justice in the digital context while addressing the privacy challenges it raises.

Data used in judicial proceedings is often made public in open courts and through published judgements and orders, as discussed in Paper I¹⁷. Court proceedings and their reporting are presumed to be open to the public, unless there are sound reasons to restrict public disclosure on grounds such as privacy, confidentiality, public safety etc. Table 1 below summarizes the provisions of the PDP Bill and the scheme of the NDP framework if they were to apply in the judicial context, highlighting how these provisions are either inadequate in protecting privacy, or are incompatible with open justice and due process. It also discusses some of our proposals on how judicial data should be regulated. Despite the exception granted to judicial functions under the PDP Bill, it is necessary to discuss the application of both the PDP Bill and NPD framework in the judicial context in order to ensure that the shortcomings of these frameworks are not replicated in the data protection framework formed for and adopted by the judiciary.



¹³ Ministry of Electronics and Information Technology (MEITY). 2019. 'Office Memorandum: Constitution of a Committee of Experts to Deliberate on Data Governance Framework.' Ministry of Electronics and Information Technology (MEITY) available online at https://www.meity.gov.in/writereaddata/files/constitution_of_committee_of_experts_to_deliberate_on_data_governance-framework.pdf (accessed on 28 December 2020)

¹⁴ Ministry of Electronics and Information Technology (MEITY). 2020. Report by the Committee of Experts on Non-Personal Data Governance Framework, available online at <https://ourgovdotin.files.wordpress.com/2020/07/kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf> (accessed on 28 December 2020)

¹⁵ Ayush Tripathi and Gautam Kathuria. 2021 Changes and challenges in the revised regulatory framework for non-personal data', 15 January, The Print, available online at <https://theprint.in/theprint-valuead-initiative/changes-and-challenges-in-the-revised-regulatory-framework-for-non-personal-data/586117/> (accessed on 04 May 2021)

¹⁶ Ministry of Electronics and Information Technology (MEITY). 2021, Draft Report by the Committee of Experts on Non-Personal Data Governance Framework: Version 2, p.18

¹⁷ DAKSH. 2021. Paper I: Balancing Open Courts with the Right to Privacy – The Indian Perspective

TABLE 1: COMPARISON OF THE PDP BILL 2019, PROPOSED FRAMEWORK FOR NON-PERSONAL DATA, AND FRAMEWORK REQUIRED FOR JUDICIAL DATA

	PERSONAL DATA PROTECTION BILL, 2019	REPORT OF COMMITTEE ON NON-PERSONAL DATA	FRAMEWORK REQUIRED FOR JUDICIAL DATA
PURPOSE	<p>The Bill is supposed to protect individual privacy in relation to personal data in general and establish a Data Protection Authority. Since much of it cannot be applied to the judicial context, Clause 36(c) specifically exempts courts and tribunals in India from significant parts of the Bill if they process data in the exercise of any judicial function, including the rights of people whom the data pertains to, and most obligations of data fiduciaries. Given the advancement of algorithms and computing, this means that data principals are exposed to considerable harm without precise and nuanced privacy regulations. The only option to protect them would be to prevent online access to judicial records, which would reduce judicial transparency considerably.</p>	<p>The objectives of the report are to formulate recommendations for the creation of economic value from data, to facilitate a data-sharing framework to make it available, and to address privacy concerns from the processing of non-personal data, including the concept of collective privacy.</p> <p>The emerging 'legal tech' industry can derive economic value from such openly available judicial data, including judicial NPD. However, not regulating such commercial use can result in negative consequences.</p>	
CATEGORIES OF DATA	<p>The categories (personal data, sensitive personal data, and critical personal data) are not directly connected to kinds and levels of harm, making balancing tests between privacy and open courts more difficult. For example, categories of information such as biometric data are more harmful than knowledge of a person's name because they enable serious harms such as fraud and identity theft, which the latter does not. These categories are also too coarse to help determine whether specific documents, data fields, and records should be made accessible to the public or to applicants who seek to use</p>	<p>NPD is defined, by exclusion, as all data other than personal data as defined in the PDP Bill. It originates either as anonymised personal data or as data that could never be traced to a specific individual. The report defines 'High Value Datasets' intended to be made available for public benefit. This does not help mediate between transparency and privacy.</p> <p>As with PDP Bill, the categories are not directly linked with harm, making them inappropriate for use in the judicial context. At present, records that would be classified as judicial NPD are available from multiple publicly accessible sources such as statistics published on court websites, e-courts</p>	<p>Regulations for judicial data should be aimed at all categories of data held by the judiciary. While broad categories such as those in the PDP Bill are useful, they could be made more so by connecting them to types and levels of harm. Other bases of categorisation could be: the type and subject matter of a case, the public interest in the disclosure of a given piece of information from the case, the quantity and granularity in which data is supplied to any applicant with a public or private interest in the information, and the relationship of any applicant to the case, if they are applying in their own private interest.</p>

TABLE 1: COMPARISON OF THE PDP BILL 2019, PROPOSED FRAMEWORK FOR NON-PERSONAL DATA, AND FRAMEWORK REQUIRED FOR JUDICIAL DATA

	PERSONAL DATA PROTECTION BILL, 2019	REPORT OF COMMITTEE ON NON-PERSONAL DATA	FRAMEWORK REQUIRED FOR JUDICIAL DATA
CATEGORIES OF DATA	<p>them for their own private interest in the judicial contest. Contextual details in judicial records often reveal personal and sensitive information even when obvious identifiers are redacted, and their removal can prevent the records from providing a coherent explanation of the adjudicatory process in a particular case.</p> <p>Critical personal data and sensitive personal data may be notified by the Central Government, which compromises judicial independence. In addition, the Central Government will not be able to know how restriction or disclosure of information could impact the fairness of judicial proceedings, which is of utmost concern in governing judicial data.</p>	<p>portal or the NJDG, and websites of certain government ministries. Treating this information as a national resource undermines the data principals' rights over a derivative of their personal information and raises numerous concerns regarding privacy and due process. It is a well-recognised fact that anonymisation is an inadequate measure to guarantee privacy. These categories are also too coarse to help determine whether specific documents, data fields, and records should be made accessible to the public or to applicants who seek to use them for their own private interest in the judicial contest. Contextual details in judicial records often reveal personal and sensitive information even when obvious identifiers are redacted, and their removal can prevent the records from providing a coherent explanation of the adjudicatory process in a particular case.</p> <p>Critical personal data and sensitive personal data may be notified by the Central Government, which compromises judicial independence. In addition, the Central Government will not be able to know how restriction or disclosure of information could impact the fairness of judicial proceedings, which is of utmost concern in governing judicial data.</p>	

TABLE 1: COMPARISON OF THE PDP BILL 2019, PROPOSED FRAMEWORK FOR NON-PERSONAL DATA, AND FRAMEWORK REQUIRED FOR JUDICIAL DATA

	PERSONAL DATA PROTECTION BILL, 2019	REPORT OF COMMITTEE ON NON-PERSONAL DATA	FRAMEWORK REQUIRED FOR JUDICIAL DATA
ROLES/ RELATIONSHIPS TO DATA	<p>The distribution of powers to access, use, share, and transform personal data in the justice system and associated responsibilities is a complex arrangement because of the specific demands of each role. These roles include judges and registry officers, as well as non-judicial actors such as police. The PDP Bill does not deal with their powers and duties in this context beyond exempting them from portions of its provisions.</p> <p>Judicial participants may also be donning multiple roles pertaining to the same information. For example, a plaintiff or their advocate may file documents containing the plaintiff's personal data, making them a principal, but they would also be a fiduciary if these documents also have the personal data of a third party, and this example merely shows the issues with the principal-fiduciary model in judicial data protection regulation.</p>	<p>The Report defines data trustees as agents of 'predetermined' communities who are tasked with protecting their data rights. Given the lack of clarity around the institutional and accountability structure of data trustees, it is not an appropriate way to govern the sharing of judicial data. Defining judicial data as public/community NPD is problematic as most of the times such data are inextricably linked to individuals. Defining a 'community' and, as a consequence choosing an appropriate 'trustee' in the context of judicial data is difficult as different groups have different competing interests on the same dataset and the NPD framework has no guidelines on how hierarchies between and within communities would be addressed. Further, if the judiciary is designated as the data trustee, it will lead to a conflict-of-interest situation where the data fiduciary and data custodian are the same.</p>	<p>The rights and obligations under this regulation should remain substantially similar to those in proposed regulations such as the PDP Bill, but numerous exceptions will need to be carved out as per individuals' role in the context of a legal case.</p> <p>For example, an accused in a criminal case cannot assert a right to deny consent to use their data. They can, however, assert other rights, such as the right for their data to be used for legal, fair, and reasonable purposes.</p> <p>In the context of judicial data, courts should retain the independence to decide what data can be made available for business/commercial purposes.</p>
RIGHTS OF DATA PRINCIPALS	<p>Data protection rights granted by the PDP Bill do not apply to the use of personal data for judicial purposes. Some rights, such as the right of access, the right to be informed, and the right to accuracy, in a limited form, would not impede court proceedings and should be retained. In addition, the Bill omits rights such as the right to object to automated processing of data, which is becoming more common in other jurisdictions.</p>	<p>The states that any person or group from which a set of NPD originates, will have rights with respect to the commercial value of that data. However, does not discuss any specific rights with respect to NPD, as far as privacy is concerned.</p>	<p>This paper proposes that privacy rights should be framed to address concerns arising from third party use of judicial data, which should be independently regulated by the judiciary.</p>

TABLE 1: COMPARISON OF THE PDP BILL 2019, PROPOSED FRAMEWORK FOR NON-PERSONAL DATA, AND FRAMEWORK REQUIRED FOR JUDICIAL DATA

	PERSONAL DATA PROTECTION BILL, 2019	REPORT OF COMMITTEE ON NON-PERSONAL DATA	FRAMEWORK REQUIRED FOR JUDICIAL DATA
OBLIGATIONS OF DATA FIDUCIARIES TOWARDS DATA PRINCIPALS	As with principals' rights, an exemption has been granted for most obligations of fiduciaries for the use of data for judicial purposes. Ideally, third parties using judicial data need to be held accountable by regulations that specify obligations beyond just lawful processing to ensure that any potential harm resulting from disclosure or processing of judicial data can be redressed.	None specified.	For judicial data, obligations would be tailored to the context in which access to the data was granted.
REGULATORY BODY	<p>The Data Protection Authority (D.P.A.) proposed in the Bill is appointed entirely by the executive branch of government.</p> <p>It has no judicial representation, and the Central Government can remove its members. The complete lack of independence from the Central Government means that if provisions related to the DPA are retained in the Bill, which is passed by parliament, judicial data should be regulated by an independent body to be free from executive interference.</p>	<p>The authority has two key goals. The first is to ensure that data is shared for public benefit and unlock the data's economic value. This cannot be the goal of privacy regulations for judicial data.</p> <p>The second goal is to ensure compliance, and to ensure that those who hold NPD respond to requests to share it. The regulations for which this authority enforces compliance are mainly directed at sharing of data for the purposes described above. This is unrelated to privacy. The only purposes for which judicial data can be forced to be shared would be when it is relevant for judicial proceedings, when a principal requests data that pertains to them, or when there is an overriding public interest to disclosure.</p>	<p>The judiciary needs a body to regulate the use of data in judicial functions and in seeking to enforce claims in court. This body would also regulate the use of data originating in judicial proceedings by third parties, since a large volume of personal data in judicial records would be made public. The members of this body must have judicial expertise other than sitting judges to avoid conflicts of interest. It also needs technical experts to assess and predict harm resulting from disclosure, particularly with regard to the fairness of the process.</p> <p>This body would also implement and administer grievance redressal mechanisms, and establish standards and protocols.</p>

TABLE 1: COMPARISON OF THE PDP BILL 2019, PROPOSED FRAMEWORK FOR NON-PERSONAL DATA, AND FRAMEWORK REQUIRED FOR JUDICIAL DATA

	PERSONAL DATA PROTECTION BILL, 2019	REPORT OF COMMITTEE ON NON-PERSONAL DATA	FRAMEWORK REQUIRED FOR JUDICIAL DATA
ROLES/ RELATIONSHIPS TO DATA	The distribution of powers to access, use, share, and transform personal data in the justice system and associated responsibilities is a complex arrangement because of the specific demands of each role. These roles include judges and registry officers, as well as non-judicial actors such as police. The PDP Bill does not deal with their powers and duties in this context beyond exempting them from portions of its provisions. Judicial participants may also be donning multiple roles pertaining to the same information. For example, a plaintiff or their advocate may file documents containing the plaintiff's personal data, making them a principal, but they would also be a fiduciary if these documents also have the personal data of a third party, and this example merely shows the issues with the principal-fiduciary model in judicial data protection regulation.	The Report defines data trustees as agents of 'predetermined' communities who are tasked with protecting their data rights. Given the lack of clarity around the institutional and accountability structure of data trustees, it is not an appropriate way to govern the sharing of judicial data. Defining judicial data as public/community NPD is problematic as most of the times such data are inextricably linked to individuals. Defining a 'community' and, as a consequence choosing an appropriate 'trustee' in the context of judicial data is difficult as different groups have different competing interests on the same dataset and the NPD framework has no guidelines on how hierarchies between and within communities would be addressed. Further, if the judiciary is designated as the data trustee, it will lead to a conflict-of-interest situation where the data fiduciary and data custodian are the same.	The rights and obligations under this regulation should remain substantially similar to those in proposed regulations such as the PDP Bill, but numerous exceptions will need to be carved out as per individuals' role in the context of a legal case. For example, an accused in a criminal case cannot assert a right to deny consent to use their data. They can, however, assert other rights, such as the right for their data to be used for legal, fair, and reasonable purposes. In the context of judicial data, courts should retain the independence to decide what data can be made available for business/commercial purposes.
RIGHTS OF DATA PRINCIPALS	Data protection rights granted by the PDP Bill do not apply to the use of personal data for judicial purposes. Some rights, such as the right of access, the right to be informed, and the right to accuracy, in a limited form, would not impede court proceedings and should be retained. In addition, the Bill omits rights such as the right to object to automated processing of data, which is becoming more common in other jurisdictions.	The states that any person or group from which a set of NPD originates, will have rights with respect to the commercial value of that data. However, does not discuss any specific rights with respect to NPD, as far as privacy is concerned.	This paper proposes that privacy rights should be framed to address concerns arising from third party use of judicial data, which should be independently regulated by the judiciary.
OBLIGATIONS OF DATA FIDUCIARIES TOWARDS DATA PRINCIPALS	As with principals' rights, an exemption has been granted for most obligations of fiduciaries for the use of data for judicial purposes. Ideally, third parties using judicial data need to be held accountable by regulations that specify obligations beyond just lawful processing to ensure that any potential harm resulting from disclosure or processing of judicial data can be redressed.	None specified.	For judicial data, obligations would be tailored to the context in which access to the data was granted.
REGULATORY BODY	The Data Protection Authority (D.P.A.) proposed in the Bill is appointed entirely by the executive branch of government. It has no judicial representation, and the Central Government can remove its members. The complete lack of independence from the Central Government means that if provisions related to the DPA are retained in the Bill, which is passed by parliament, judicial data should be regulated by an independent body to be free from executive interference.	The authority has two key goals. The first is to ensure that data is shared for public benefit and unlock the data's economic value. This cannot be the goal of privacy regulations for judicial data. The second goal is to ensure compliance, and to ensure that those who hold NPD respond to requests to share it. The regulations for which this authority enforces compliance are mainly directed at sharing of data for the purposes described above. This is unrelated to privacy. The only purposes for which judicial data can be forced to be shared would be when it is relevant for judicial proceedings, when a principal requests data that pertains to them, or when there is an overriding public interest to disclosure.	The judiciary needs a body to regulate the use of data in judicial functions and in seeking to enforce claims in court. This body would also regulate the use of data originating in judicial proceedings by third parties, since a large volume of personal data in judicial records would be made public. The members of this body must have judicial expertise other than sitting judges to avoid conflicts of interest. It also needs technical experts to assess and predict harm resulting from disclosure, particularly with regard to the fairness of the process. This body would also implement and administer grievance redressal mechanisms, and establish standards and protocols.

HOW SHOULD JUDICIAL DATA BE REGULATED?

The key issues in regulating judicial data result from the digitisation of both court records and the processes that support judicial proceedings. It is therefore necessary to briefly discuss court digitisation initiatives in the Indian judiciary, and how these have altered access to judicial data.

Paper I established that the documents and data which are currently publicly accessible include copies of judgments, orders, and cause lists¹⁸. At present, the E-Courts Mission Mode Project, led by the eCommittee of the Supreme Court of India, is in Phase II, and is in the process of planning Phase III. Phases I and II have resulted in courts beginning to upload judgments, orders, and cause lists to the E-Courts portal and mobile application. These channels also provide other information as separate data fields¹⁹. These include the names of litigants and their advocates, judges, details of the court and court hall, the type of case, and the laws under which the case was filed, the status of the case, and its outcome once it has been disposed of²⁰. Digitising existing physical records is also a part of the E-Courts project²¹.



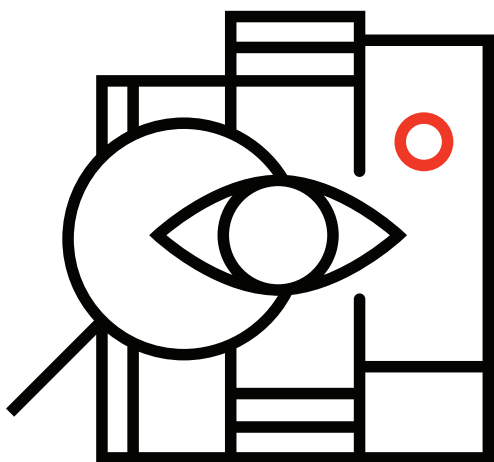
¹⁸ DAKSH. 2021. Paper I: Balancing Open Courts with the Right to Privacy – The Indian Perspective

¹⁹ eCommittee Supreme Court of India. 2016. 'Case Management Through CIS 3.0 (Case Information system 3.0)', E-Courts, pp. 199-209, available at https://ecourts.gov.in/ecourts_home/static/manuals/Case%20Management%20through%20CIS%203.0.pdf

²⁰ eCommittee Supreme Court of India. 'Case Management Through CIS 3.0 (Case Information system 3.0)'

²¹ E-Committee, Supreme Court of India. 2019. eCourts Project Phase II Objectives Accomplishment Report

As per Policy Action Plan Document, Delhi: Supreme Court of India. E-Courts. Available at https://ecourts.gov.in/ecourts_home/static/manuals/Objectives%20Accomplishment%20Report-eCourts-final_copy.pdf



At present, these digital records are not ‘machine readable’, meaning that they have been designed for humans to read, and not for processing by a computer²². This means that specialised computational techniques which are adapted to extracting information from court records would be necessary to extract specific fields or classes of information from these records²³. Compiling and aggregating the information currently available requires considerable effort, and has been done through a process of information extraction known as ‘scraping’²⁴. This process has been used to analyse court performance²⁵ and make court records more easily searchable²⁶. Releasing data which can be analysed therefore serves an important role in increasing the transparency and accountability of the judiciary. However, the increase in access to records, and the scope for aggregation and combination of datasets, has upset the balance between transparency and privacy which had previously been established by the judiciary in the physical context²⁷. There is therefore a need to ensure that this information can remain publicly accessible while minimising the risks associated with doing so in the digital context.

A draft plan for Phase III of the E-Courts project proposes to make documents machine readable, and to make data publicly accessible via ‘Application Programming Interfaces’ (APIs), which are standardised instructions for different computer systems to communicate with one another²⁸. While this greatly increases the ways in which information can be accessed and used, it also exacerbates the risks of aggregation by enabling programs and applications to more easily access data. This results in a subversion of the practical limits on the usability of judicial data that exist in current digital systems. The implementation of regulations, protocols, and design practices which appropriately address the concerns that result from digitisation of access is needed to restore the balance between open justice and privacy that was established in the physical context without obstructing the modernisation of judicial information systems. The subsequent sections therefore address privacy concerns in remote access to digital judicial records, both in the present context, as well as in a potential future in which these objectives have been achieved.

²² Charles M. Dollar. 1978. ‘Appraising machine-readable records.’ *The American Archivist* 41(4): 423-430.

²³ These include ‘Natural Language Processing’ (NLP); see Mauro Dragoni, Serena Villata, Williams Rizzi, and Guido Governatori. 2016 ‘Combining NLP approaches for rule extraction from legal documents.’ In 1st Workshop on Mining and Reasoning with Legal texts (MIREL 2016)

²⁴ DAKSH. 2020 ‘Deciphering Judicial Data: DAKSH’s Database’ DAKSH. Available at <https://dakshindia.org/wp-content/uploads/2020/08/Case-categorization-paper-FINAL.pdf>; Rahul Hemrajani and Himanshu Agarwal. 2019. ‘A temporal analysis of the Supreme Court of India’s workload’ *Indian Law Review* 3(2): pp. 125-158, available online at <https://www.tandfonline.com/doi/full/10.1080/24730580.2019.1636751>; Devendra Damle and Tushar Anand. ‘Problems with the e-Courts data.’ 2020. National Institute for Public Finance and Policy, No. 20/314, Available online at https://www.nipfp.org.in/media/medialibrary/2020/07/WP_314__2020.pdf

²⁵ Kishore Mandyam, Harish Narasappa, Ramya Sridhar Tirumalai and Kavya Murthy. 2016. ‘Chapter 1: Decoding Delay: Analysis of Court Data’, in Harish Narasappa & Shruti Vidyasagar (eds), *The State of the Indian Judiciary: A Report by DAKSH*, Bengaluru: DAKSH, available online at http://dakshindia.org/state-of-the-indian-judiciary/11_chapter_01.html#_idTextAnchor009

²⁶ For example, see Indian Kanoon, available online at <https://indiankanoon.org/>

²⁷ DAKSH. 2021. Paper I: Balancing Open Courts with the Right to Privacy – The Indian Perspective

²⁸ Expert Sub-Committee to draw up a Vision Document for Phase III, E-Committee of the Supreme Court of India. 2021. Draft Digital Courts Vision & Roadmap Phase III of the eCourts Project, E-Committee of the Supreme Court of India, available online at <https://cdnbbsr.s3waas.gov.in/s388ef51f0bf911e452e8dbb1d807a81ab/uploads/2021/04/2021040344.pdf> (accessed on 1 May 2021)

A. CRITERIA FOR CARVING OUT EXCEPTIONS TO THE OPEN COURTS DOCTRINE ON GROUNDS OF PRIVACY

Since the open courts doctrine will be the default policy that is applied in the judicial context, data regulations should address privacy concerns by carving out exceptions to it. These can be arrived at through the use of multiple criteria to apply limited restrictions to the release of data. Some broad principles which can guide the formulation of such a policy are described below²⁹.

1. The key to developing policy for both civil and criminal justice information is to consider “content and context”

Information contained in judicial records must be considered by its type, as well as the context in which it appears. Information contained in judicial records can be “large or small,” such as a personal identifier (name) or the sum of many elements (i.e., documents, such as arrest reports, indictments, pleadings, court orders).

Where possible, privacy policies must be applied to each data element in the judicial records. Additionally, each element needs to be considered in context. For example, general information describing dates, places, and events may be deemed disclosable between courts and other agencies like police, prisons, etc., and to the public. If this information is contained in a document in an ongoing investigation, however, if there is a threat to the safety of a victim, witness, or the public, it may not be publicly accessible until the

investigation is concluded. Similarly, a data element such as ‘address’ may be deemed disclosable or publicly accessible, generally. If, however, the address is that of a victim and appears in the victim statement or a court exhibit, a privacy analysis may determine that it is not suitable for inter-agency sharing and probably not appropriate for public access.

2. Data regulations must recognise the relationship of an individual with the justice system

Within the context of judicial proceedings, it may be helpful to consider regulations that cater to three audiences:

- Internal, meaning those individuals and agencies within the justice system: law enforcement, prosecutors, defence counsel, judges, court administration, correctional facilities, vendors who provide technological services to the judiciary (whose contractual obligations must also include their adherence to privacy regulations and associated liabilities); and
- External, meaning those actors (e.g., charged or convicted offenders, plaintiffs, witnesses, or victims) who have a relationship with the justice system but are not an operational part of the system.
- The public, meaning individuals or groups with no relationship or participation in proceedings, which would include citizens, civil society, journalists, academic researchers, and firms in the emerging legal tech industry.

Issues specific to each of these audiences need to be addressed within judicial data regulations. One must note that when considering the “internal” audience, there is a tendency to assume a free flow

of personal information relating to anyone with a “relationship” to the justice system, as long as the sharing is done for stated and lawful purposes. Existing rules for sharing information within the criminal justice system (e.g., police, prosecutors, defence, courts, and corrections) would differ from rules used to determine the disclosure of that information to parties outside the justice system. For example, evidence collected by police or investigation agencies would need to be shared with public prosecutors, the accused, and their lawyer; but these are generally not made public.

²⁹ National Criminal Justice Association. 2002. ‘Justice Information Privacy Guideline – Developing, Drafting and Assessing Privacy Policy for Justice Information Systems’, National Criminal Justice Association, September, available online at https://it.ojp.gov/documents/ncisp/privacy_guideline.pdf (accessed on 30 December 2020); Martha Wade Steketee and Alan Carlson. 2002. ‘Developing CCJ/COSCA Guidelines for Public Access to Court Records: A National Project to Assist State Courts’, The National Center for State Courts and The Justice Management Institute, available online at <https://ncsc.contentdm.oclc.org/digital/collection/accessfair/id/210/> (accessed on 30 December 2020)

3. Judicial data regulations must recognise the status/ role of an individual in the justice system

Individuals whose privacy interests may be affected by the courts processing their data include victims, witnesses, law enforcement officers, judges, court staff, plaintiffs, respondents, lawyers/advocates, defendants, offenders, families and associates of these persons, and anyone who comes in contact with the judicial process. Judicial data regulations must be mindful of the various types of interactions these individuals have with the courts, and how their personal information is collected and intended to be used in the judicial process. For example, a convicted criminal's personal information would be dealt with differently than a witness's personal information. Furthermore, treatment of personal information collected for investigation may differ from information collected and used in a case processing system³⁰.

This section provides an indicative framework for access to court records by various stakeholders based on their role, function, and relationship with the justice system. Other factors include the sensitivity and granularity of information requested. This section also highlights the responsibilities of the courts, which are the custodians of all information provided by the judicial participants.

B. THE BASIS FOR DETERMINING THE EXTENT OF PRIVACY PROTECTIONS AND PUBLIC ACCESS GRANTED TO JUDICIAL DATA

Any regulation governing judicial data must provide for a means of balancing the public interest in making judicial data widely available, and privacy concerns associated with it, as objectively and consistently as possible. This can be achieved by accounting for all of the data's characteristics that bear on the demands for privacy, transparency, or both. In certain situations, specific to judicial proceedings, both privacy concerns and transparency requirements emerge from the context of the usage of the information, rather than just the content of the information in isolation. An overview of these factors is given below.

1. Sensitivity of data fields

Many privacy frameworks, from the PDP Bill to the GDPR, specify broad classes of data based on their sensitivity³¹. The sensitivity of data is determined based on the degree of harm that a person is exposed to as a result of the public disclosure of such data. Privacy laws from various jurisdictions demarcate personally identifiable information, or PII (information that enables identification of a natural person) as meriting protection because its use in certain circumstances can amount to an invasion of privacy³². Many offer a higher degree of protection to a class of 'sensitive personal data'³³, which exposes the subject of that data to a much higher degree of threat if revealed. Demarcating categories of data based on the potential vulnerability of the principal provides an easy, consistent way of weighing privacy against transparency. This will be essential to regulate the access and ensure transparency as the judiciary moves to natively digital processes³⁴. Hence, we discuss the relevance of identifiers and harm in formulating judicial data regulations, and how they would need to be modified so that they do not impact the open courts doctrine.

³⁰ See Clause A. 2. Of Chapter 3 on roles as defined in the PDP Bill, 2019

³¹ General Data Protection Rights, the PDP Bill, and other laws such as the United Kingdom's prior Data Protection Act, the California Consumer Privacy Act in the United States of America.

³² Clause 3 (36), PDP Bill 2019; Article 9, General Data Protection Regulation

³⁴ DAKSH. 2019. Whitepaper Series on Next Generation Judicial Platform, Paper 3: Legal Framework. Bengaluru: DAKSH, available online at https://dakshindia.org/wp-content/uploads/2020/02/Paper-3_Legal-Framework.pdf (accessed 30 December 2020)

i. Open data – by default

To begin with, it is necessary to designate a class of open data within which the potential for harm or misuse is negligible. This includes categories of information and records that will be made public, such as statistics on the judiciary, its policies, rules, and most administrative information which does not relate to personal and sensitive aspects of individual staff members. It should also include all information from judicial records which does not contain sensitive information, or documents and other records from which all information with scope for misuse has been removed. This should include judgments and orders after removing sensitive personal data, and identifiers for bulk data. While non-sensitive personal data would not typically be thought of as safe to include in open data, open justice demands that some kinds of PII would need to be designated as open data, based on the context and volume in which it is made available. These factors are discussed below.

It is essential that access to open data should not require an application process, and that people and institutions who use it do not need to obtain permission or prove their need to access it³⁵. Designating a class of information as open to the public creates an obligation to disclose it and minimises the circumstances for limiting access to this information (i.e. the default rule is that the class of open data is publicly accessible).

ii. Personal data (PD)

The link between a unit of data and a natural person is also the basis of that person's rights with respect to

the data. Since privacy is a means of safeguarding an individual's dignity, their rights become applicable when data is associated with their identity. However, using identifiability alone as a primary criterion for curtailing access to information under the open courts doctrine is problematic. The concept of personally identifiable information as a category for data protection regulation is useful, but should not be the primary basis of regulation in the judicial context.

In multiple judgments, the Supreme Court and many High Courts have ruled on the need to weigh the public interest in obtaining information against the privacy of those it pertains to in the context of RTI applications³⁶. Making personal data public as per the open courts doctrine cannot be regarded as a violation of the fundamental right to privacy, as it is congruent with the principles set out in the Puttuswamy judgment. It fulfils the criteria that the Supreme Court established for legitimate curtailment of the right to privacy, which are legality, necessity, and proportionality³⁷. The legality criterion is fulfilled by provisions of the Code of Civil Procedure, 1906, and the Code of Criminal Procedure, 1971, which require the place of trial³⁸, hearing of evidence of witnesses³⁹, and pronouncements of judgments⁴⁰, to generally be held in an open court. Article 145(4) of the Constitution requires that Supreme Court's judgments be pronounced in open court. Regarding necessity, releasing data in the interest of the fair administration of justice passes the test proposed in the Puttuswamy judgment. The curtailment of the right to privacy must serve a legitimate state interest⁴¹.



³⁵ Martha Wade Steketee and Alan Carlson. 2002. 'Developing CCJ/ COSCA Guidelines for Public Access to Court Records: A National Project to Assist State Courts', The National Center for State Courts and The Justice Management Institute, available online at <https://ncsc.contentdm.oclc.org/digital/collection/accessfair/id/210/> (accessed on 30 December 2020)

³⁶ Girish Ramchandra Deshpande vs. Central Information Commissioner (2012), Special Leave Petition (Civil) No. 27734 of 2012; Subhash Chandra Agarwal v. Registrar, Supreme Court of India LPA 34/2015 and C.M. No. 1287/ 2015, High Court of Delhi, April 17, 2015; CPIO, Supreme Court of India v. Subhash Chandra Agarwal, Civil appeal no. 10044 and 2683 of 2010, Supreme Court of India, November 13, 2019.

³⁷ DAKSH. 2021. Paper I: Balancing Open Courts with the Right to Privacy – The Indian Perspective

³⁸ Section 153B of the Code of Civil procedure (CPC), 1906; section 327 of the Code of Criminal Procedure (CrPC) 1971

³⁹ Sections 274, 275, and 276.

⁴⁰ Section 265F of the Code of Criminal Procedure (CrPC)

⁴¹ K.S. Puttuswamy v. Union of India, Writ Petition (Civil) No. 494 of 2012, Supreme Court of India, Justice D.Y. Chandrachud for himself and Justice Jagdish Chandra Kehar, Justice R.K. Agrawal and Justice S. Abdul Nazeer DAKSH. 2021. Paper I: Balancing Open Courts with the Right to Privacy – The Indian Perspective

Personal data should only be included within documents accessible to the public to the extent that the data itself is a fact used by a judge to reach a judicial decision. For example, the address of a victim of a crime may not in itself be relevant to their decision in a particular case, but the fact that the accused knew this address or lived in the same street may be relevant. In this example, there would be no reason to include the address itself in the publicly accessible documents associated with proceedings, such as orders and judgments. This principle cannot be translated directly into policy, but could be factored into privacy-related training that is given to judges and court staff.

Given the fact that the identity of litigants is an integral part of judicial records, identifiability within a public document itself, should not be used as the main criterion for restriction on grounds of privacy. Privacy-based restrictions of access to information in court records should be based on the probability of a piece of information being used to cause undue harm to the data principal, and the nature and magnitude of that harm. If information system design can ensure that un-redacted judgments and orders can only be accessed on a case-by-case basis, this information should therefore not be redacted from the public record unless it meets the sensitivity criteria, or pertains to sensitive subject matter.

“

The presence of personal identifiers in publicly accessible bulk records, however, is qualitatively different given the heightened potential for harm. If court records are made machine readable and accessible via API, markup language should be used to tag the personal identifiers contained within such records such that they can be automatically redacted, before being made available to the public.

”

iii. Sensitive personal data (SPD)

Specific exceptions to the open courts doctrine should be created for a more protected class of data. This category must be demarcated based on whether the data could expose data principals to an elevated degree of harm. The types of data included under sensitive personal data in the PDP Bill should be in this category by default – these include financial information, medical and health-related information, official identifiers, and biometric and genetic data, but the scope of what is designated as sensitive data should not be restricted to these strictly defined categories. The designation of data as sensitive should be closely connected with the harm that it exposes the subject to, and such determination should be made by judiciary, possibly through an independent judicial data regulator.

Given that many of the privacy risks associated with a piece of data are contextual, it is likely that sensitive information may emerge through understanding the role of that information in the context of a case, rather than in isolation. Thus, framing the boundaries of sensitive personal data in terms of types of potential or actual privacy harm, and devising tests for these harms, is essential to give practical value to the data rights conferred upon litigants and their lawyers under such a framework. For example, if a lawyer requests that a portion of a document be redacted from the publicly accessible version of the document, a consistent means of evaluating the potential privacy harm resulting from public disclosure would help reduce ambiguity in these circumstances. It would simultaneously prevent the subjective and contextual element of privacy risk from denying people protection.

An important step which the regulatory framework will have to take will be making the leap from document-based regulations to data field-based regulations.

Table 2 below illustrates the nature of personal information, and potentially sensitive information, in a limited selection of judicial documents. It also includes documents prepared by other entities that play a key role in proceedings, such as charge sheets prepared by the police. Personal and sensitive personal information and associated privacy risks exist in many documents of public nature. These documents cannot simply be removed from the public domain because they pose a privacy risk. In such a situation, a data field-based approach, rather than a document-based approach, may be more effective and precise at preserving open judicial data while preventing privacy harms. Where currently possible, such as for case information made available on the E-Courts portal other than orders and judgments⁴⁵, field-based regulations can be implemented. Both privacy risks posed by specific data fields, as well as means to address them through systems design, would be much greater for marked up judgments and orders.

⁴² Daniel J. Solove. 2005. 'A Taxonomy of Privacy', University of Pennsylvania Law Review, 154: 477.

⁴³ Iohannis Agrafiotis, Jason RC Nurse, Michael Goldsmith, Sadie Creese, and David Upton. 'A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate', Journal of Cybersecurity, 4(1): ty006

⁴⁴ Bert-Jaap Koops, Bryce Clayton Newell, Tjerk Timan, Ivan Škorvánek, Tomislav Chokrevski, And Maša Galič. 2017. 'A typology of privacy', University of Pennsylvania Journal of International Law, 38(2): 483-575

⁴⁵ eCommittee Supreme Court of India. 2016. 'Case Management Through CIS 3.0 (Case Information system 3.0)', E-Courts, p. 204, available at https://ecourts.gov.in/ecourts_home/static/manuals/Case%20Management%20through%20CIS%203.0.pdf

Table 2 broadly illustrates the personal and sensitive personal data found in various categories of court records and the current extent as well as means of public access to such records. However, it must be borne in mind that this table is merely a starting point and not not exhaustive of all kinds of privacy risks that may arise. Since privacy and privacy risks are highly contextual, a broad mapping like the one below is insufficient to chalk out the privacy concerns in each context. Instead, a large-scale information flow mapping exercise, followed by an assessment of the probability and magnitude of harm resulting from privacy violations, should be conducted to account for contextual factors. Some factors that can be used to determine if the data is sensitive are⁴⁶:

1. the capability of data to be used to inflict harm (ranging from fraud to social discrimination);
2. the probability of this occurring if the data is publicly disclosed;
3. the expectation of confidentiality regarding certain types of data, such as health data; and
4. concerns expressed by a majority of citizens, which are relevant since the harms which do occur only affect a minority of the population, meaning that the majority is less likely to be concerned with those specific harms.

In the present context, a procedure should be implemented for lawyers to seek removal of this information from the online public record. The court should retain the discretion to determine, either of its own motion or upon request by a party, that the public interest in having access to particular piece of sensitive data outweighs the privacy risks and the data should therefore not be redacted. As with PD, if court records are ever made machine readable and made accessible via API, court information systems, markup language should be used to tag sensitive information that is identified as such by lawyers at the time of filing, enabling automated redaction.

⁴⁶ Paul Ohm. 2014. 'Sensitive information.' *Southern California Law Review*, 88:1125.

TABLE 2: DATA FIELDS PRESENT IN DIGITAL COURT RECORDS

DOCUMENT	CURRENT EXTENT AND MEANS OF PUBLIC ACCESS IN INDIA	EXAMPLES OF PERSONAL DATA WITH ELEVATED PRIVACY RISKS, WHICH SHOULD BE REGARDED AS SENSITIVE DATA	OTHER PERSONAL DATA
JUDGMENT/DECREE	Publicly accessible (as defined earlier) except for specific examples such as in cases of domestic violence, divorce, or under the Protection of Children from Sexual Offences (POCSO) Act, 2012, or if ordered by the court.	Information pertaining to minor children which cannot be removed through redaction of specific identifiers, medical information, sensitive financial information, classes of educational information, facts enabling identification and other forms of harm to vulnerable witnesses such as their addresses, information relating to sensitive matters such as family relationships in contexts where proceedings may still be open to the public, such as in intra-family property disputes, and information which is not risky when viewed in isolation, but which can be aggregated with other public information to interfere with a person's life, ID numbers,	Names of parties, lawyers, and judges, names of witnesses in minor matters in which they are not vulnerable, details of ownership of movable and immovable property, employment information, details of parties' and lawyers' actions during proceedings, non-sensitive details of professional, social, and familial relationships, non-sensitive descriptions of the character of parties, descriptions of parties' claims and events which play a key role in the decision, and details of facts and evidence which the judge relies on
INTERIM ORDERS			

TABLE 2: DATA FIELDS PRESENT IN DIGITAL COURT RECORDS

DOCUMENT	CURRENT EXTENT AND MEANS OF PUBLIC ACCESS IN INDIA	EXAMPLES OF PERSONAL DATA WITH ELEVATED PRIVACY RISKS, WHICH SHOULD BE REGARDED AS SENSITIVE DATA	OTHER PERSONAL DATA
LIVE STREAMING OF PROCEEDINGS	Publicly accessible (as defined earlier) except for specific examples such as in cases of domestic violence, divorce, or under the Protection of Children from Sexual Offences (POCSO) Act, 2012, or if ordered by the court.	Same as above but also including logs on usage of the platform by parties, lawyers, judges, court staff, witnesses, and other attendees, as well as data which may expose attendees to cyber risks, details of charges or issues as read out in court and personal data revealed during witness examination and cross-examination (if the subject matter or personal data is sensitive)	Same as above but also including logs on usage of the platform by parties, lawyers, judges, court staff, witnesses, and other attendees, details of charges or issues as read out in court and personal data revealed during witness examination and cross-examination (if the subject matter and personal data is not sensitive)
INFORMATION HOSTED ON E-COURTS PORTAL AND ASSOCIATED APPS (INCLUDING E-FILING, E-PAY, AND OTHER ALLIED ONLINE JUDICIAL SERVICES)		Potentially sensitive data available in interim orders and judgments, as well as logs on parties' and lawyers' use of digital judicial services	Details of hearings dates, appearances of parties' names in cause lists, and purposes of hearings

TABLE 2: DATA FIELDS PRESENT IN DIGITAL COURT RECORDS

DOCUMENT	CURRENT EXTENT AND MEANS OF PUBLIC ACCESS IN INDIA	EXAMPLES OF PERSONAL DATA WITH ELEVATED PRIVACY RISKS, WHICH SHOULD BE REGARDED AS SENSITIVE DATA	OTHER PERSONAL DATA
FIR AND PRIVATE COMPLAINTS	Accessible through application under RTI. Act, although the request may be denied.	ID numbers of the complainant and/or victims and witnesses, details of the alleged offence if the matter is sensitive or if sensitive information is necessary to establish the facts of the offence (e.g., information on bodily injury would be seen as medical data, which is highly sensitive, or financial data in the case of fraud), signatures of victim or complainant, any witnesses, and investigating officer or any other officer who receives the complaint	Names, addresses, phone numbers, and other contact data of accused, complainant and/or victims, family members (such as father/husband), information on the location of and events surrounding the alleged offence, name of the police officer who received the complaint/F.I.R., names and similar contact details of witnesses if known
CHARGE SHEET		Same as for F.I.R., with the addition of further potentially sensitive data of the accused and witnesses, such as official I.D.s, financial data, forensic, genetic, and biometric data,	Same as for FIR with the addition of provisional number identifying the case, details of arrest and remand or bail, name and contact information of person providing sureties, relevant events of IOO's investigation excluding any sensitive data, list of charges and statutory punishment under Indian Penal Code, 1860, details regarding ownership, use, or damage to property if relevant, religion, details of previous convictions of accused

TABLE 2: DATA FIELDS PRESENT IN DIGITAL COURT RECORDS

DOCUMENT	CURRENT EXTENT AND MEANS OF PUBLIC ACCESS IN INDIA	EXAMPLES OF PERSONAL DATA WITH ELEVATED PRIVACY RISKS, WHICH SHOULD BE REGARDED AS SENSITIVE DATA	OTHER PERSONAL DATA
EVIDENCE EXHIBITS		information of vulnerable witnesses and victims, detailed original financial records containing data that expose the data principal to significant personal risk, and intellectual property which merits protection.	including public records, expert witness opinions, facts that link exhibits to the case, details of ownership of exhibits.

2. Balancing sensitivity of data fields against precedent value and overriding public interest

The point above recommended that courts should have discretion over the public disclosure of SPD in court records. This part will discuss principles and tests which can aid these decisions.

There are numerous examples of the judiciary restricting or preventing disclosure of SPD in court records to protect both individual privacy and fair administration of justice⁴⁷. These can help ensure that a curtailment of privacy necessary to achieve fair administration of justice is proportionate and balanced. Consistent, codified, 'bright line' tests of proportionality, however, are much more difficult to devise, given how contextual both privacy and the trade-off between privacy and transparency can be. For example, consider an example where the information pertains to intimate details of a person's private life, in which they are alleged to have committed some minor crime. If that information is evidence in the case which is described in a judgment, there would be sufficient public interest to disclose it if disclosure would simply be mildly embarrassing for the party, but not if it would result in a serious and credible threat of violence against them.

Much of the determination of privacy protection should depend on an assessment of potential harm using the sensitivity described above. Tests of proportionality for public disclosure of judicial data from an open courts perspective could be based on the extent of

broader, societal harms that would result from a case being decided unfairly, with particular regard to the impact not only on parties unfairly punished but also on society at large, especially where the decision is binding on other courts. This could perhaps be achieved by defining levels of public interest that override privacy concerns for each level and type of harm, as described earlier. The level of public interest that applies to a given case could be determined by assessing the fulfilment of specified criteria.

One approach proposed by Amanda Conley, Anupam Datta, Helen Nissenbaum & Divya Sharma involves balancing the public need for access to court documents, the extent of previous access to these documents, claims of property and privacy rights associated with the data, potential prejudice to those opposing disclosure, and the purposes for which those documents were made part of the record⁴⁸. Peter Winn recommends expanding the use of a test established by the US Court of Appeals for the Third Circuit in *Westinghouse Electric Corp. v. United States*⁴⁹, which originally was used to decide on the balance between privacy and the need for disclosure of health records in service governmental objectives⁵⁰. The *Westinghouse* test has three factors similar to those in the model provided in Conley et al.; the need for access, the potential for harm resulting from disclosure, and the nature of the information contained in it. However, it differs in that it mentions the adequacy of security safeguards and the effect of disclosure on the relationship which produced the record as being the additional factors.

⁴⁷ DAKSH. 2021. Paper I: Balancing Open Courts with the Right to Privacy – The Indian Perspective, Naresh Sridhar Mirajkar v. State of Maharashtra, AIR 1967 SC 1

⁴⁸ Amanda Conley, Anupam Datta, Helen Nissenbaum & Divya Sharma. 2011. 'Sustaining Privacy and Open Justice in the Transition to Online Court Records: A Multidisciplinary Inquiry,' Maryland Law Review, 71: 722

⁴⁹ *Westinghouse Electric Corp. v. United States*, 466 U.S. 388 (1984)

⁵⁰ Peter A Winn, 2004. 'Online court records: Balancing judicial accountability and privacy in an age of electronic information,' Washington Law Review, 79: 307.

While these tests are broad enough to enable the interpretation of their underlying principles in the context of reaching a judicial decision on privacy in court records, a more precise test is necessary to make consistent decisions. These tests are also document-based, which may be adequate for the present extent of digital access to orders and judgments, but would be inadequate for a future of marked up documents and bulk access via API.

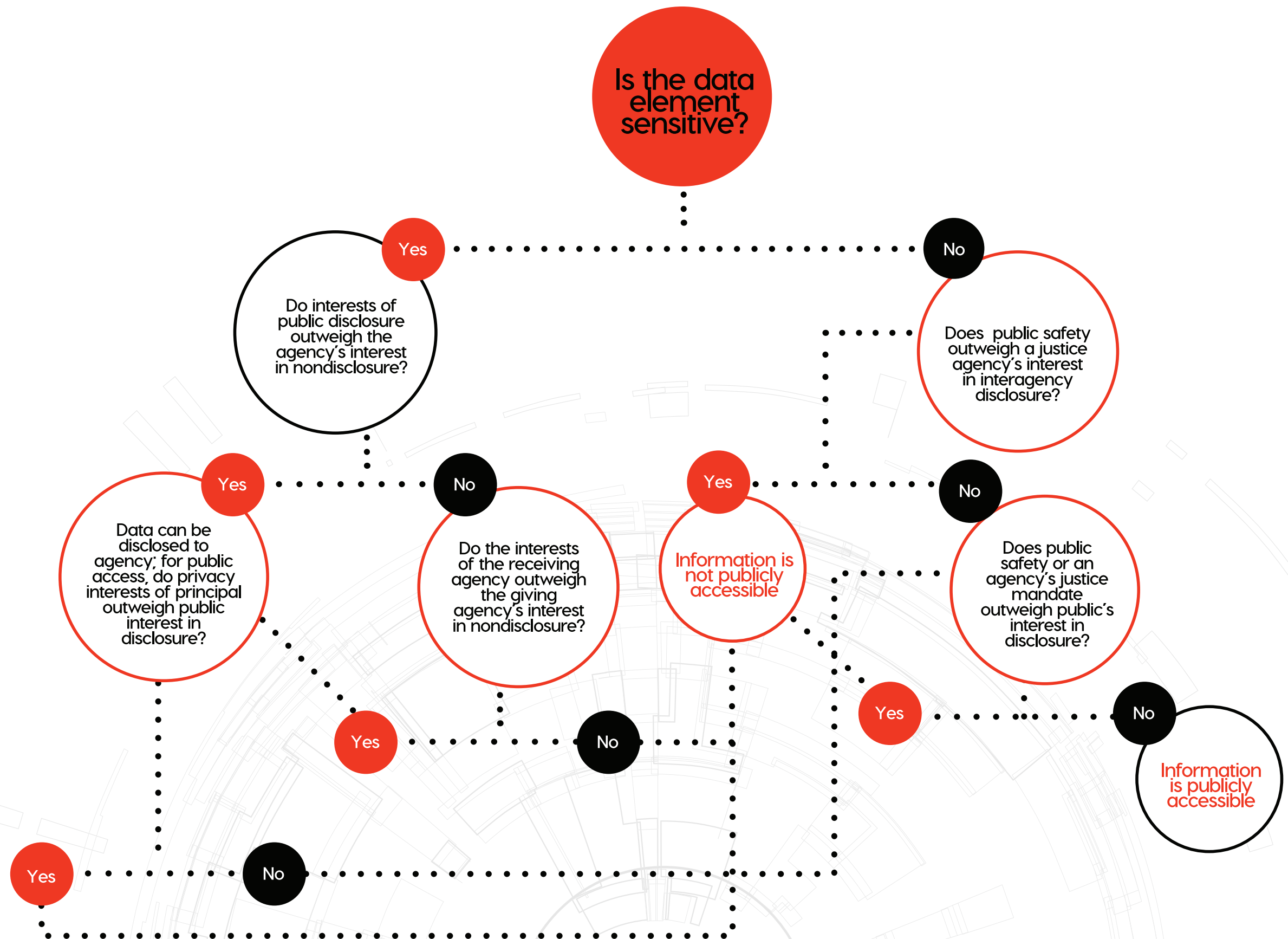
For both the present and this potential future, an approach suggested by the ‘National Criminal Justice Association’ in the USA⁵¹ may be more useful. They propose a 5-stage test for determining whether the information is either non-disclosable, disclosable only on request and after consideration of consequences, or public by default. They refer to these three levels as ‘red’, ‘yellow’, and ‘green’, respectively. This test requires answering a sequence of questions, as depicted in Figure 1.⁵²



⁵¹ National Criminal Justice Association. ‘Justice Information Privacy Guideline – Developing, Drafting and Assessing Privacy Policy for Justice Information Systems’

⁵² National Criminal Justice Association. ‘Justice Information Privacy Guideline – Developing, Drafting and Assessing Privacy Policy for Justice Information Systems’, p.64.

FIGURE 1: BALANCING SENSITIVITY AGAINST PUBLIC INTEREST – NCJA APPROACH



3. Case type and subject matter

Indian courts already carve out exceptions to the open courts doctrine and the right to privacy based on the subject matter of cases. Courts hold in-camera trials in these cases, either compulsorily as mandated by various statutes or as per the judge's discretion. Divorce and matrimonial cases, cases under the Protection of Children from Sexual Offences (POCSO) Act or Protection of Women from Domestic Violence Act, cases on rape, sexual assault, or cases involving minors are examples where courts do not have to make information related to the court proceedings public.

If the judiciary implements marked up court documents and makes them accessible via API, regulations can allow more transparency. Case type, in combination with other factors and conditions, may be used to determine parts of the record that would not ordinarily be open to be included in the publicly accessible records. For example, some personal identifiers that would not otherwise be publicly accessible, may be legitimately made public in writ petitions or on matters of significant constitutional importance, or case types specifically concerning the conduct of public officials.

4. Granularity

The volume of data that is made available has a bearing on both the potential benefits it can deliver, and its potential for misuse. These risks are largely unique to the digital context, resulting from the loss of practical obscurity. With paper records, there are obvious physical constraints that prevent

people from efficiently accessing, aggregating, and processing information in bulk. In addition, increases in computational power have enabled processing of bulk data in ways that were previously impractical. The open courts doctrine does not address bulk access, given that it evolved in a context of paper records.

Aggregation and processing of information in bulk, mainly through the use of recently developed machine learning algorithms, exposes individuals to harm that is both quantitatively and qualitatively different. It renders anonymised data re-identifiable⁵³, and makes people vulnerable to profiling, which can be used to both make predictions regarding their lives and surreptitiously influence their decisions⁵⁴. However, there are significant benefits to transparency that can be achieved by regulating the granularity of the information that is made available. Refer to Annexure 1. The ongoing digitisation of judicial records provides an opportunity to do so⁵⁵. We therefore, propose that the mode and quantity in which judicial data is made available should be adapted to the inherent sensitivity of given types of information, case type, and context.



⁵³ Aurelia Tamò-Larrieux, Tamò-Larrieux, and Seyfried. 2018. 'Designing for privacy and its legal framework'. Cham: Springer

⁵⁴ Carole Cadwalladr and Emma Graham-Harrison. 2018. 'Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach', The Guardian, 17 March, available online at <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> (accessed on 30 December 2020)

⁵⁵ DAKSH, Whitepaper Series on Next Generation Judicial Platform, Paper 3: Legal Framework.

i. Case-by-case/ individual case level access

Access to specific records on an individual basis, using technological tools to monitor traffic, can be used to regulate access to judicial records. Providing bulk access to some types of information can expose people to harms that would not result from access to records from individual cases, one-at-a-time. As Solove observes, aggregation and re-combination of data will 'render the whole greater than the sum of its parts.' Profiling and other risks that emerge from the use of machine learning and allied technologies depend on data being available in large volumes to train algorithms. Providing access to a data point at an individual case level while preventing such data points from being available in bulk quantities would ensure that the core principles behind open courts, namely fairness of the judicial procedure, are fulfilled while minimising the chances of misuse of such information. Therefore, public documents that contain PD, such as orders and judgments, should only be made individually accessible.

ii. Bulk Access

Bulk access, in this context, refers to the ability to access data from multiple cases in which individual cases can be identified. Despite the risks mentioned above, providing bulk access to certain data points is necessary for many uses and can serve valuable purposes. However, given the risks of bulk access, it should be provided only to the extent necessary for these useful applications. Bulk access to de-identified data of the kind that is available on the E-Courts portal in webpage form, which captures information

on subject matter, hearing dates and purposes, and outcomes of cases, can be made available to the general public, as it plays a significant role in both academia and civil society.

Bulk access to judgments and orders presents a greater obstacle given the privacy risks that this would entail. For specific kinds of subject matter, such as government litigation, writ petitions, and other subject matter of great public importance, could be granted, provided that they can be identified using present data fields in the Case Information System (CIS) software that courts use in case management⁵⁶. The lack of machine readable, marked up legal documents, including judgments and orders, mean that making all judgments and orders available in bulk should be prevented until technical development reaches this stage. Once this stage is reached, however, automated redaction of identifiers would make this much safer. Third parties who are granted access to un-redacted bulk data, must take on additional obligations and be subject to strict monitoring, and the purposes for which they may be granted permission to do so must be strictly limited.

iii. Aggregates

Aggregate data results from applying quantitative or other analytical techniques to bulk data, providing some information about the group that constitutes the data set of the bulk data. It summarises some detail about the group but does not enable the identification of individuals within the group. One such example is the data hosted on the NJDG, which provides information on case duration and pendency.

The advantage of aggregate statistics is that they can be used to summarise information about events that would otherwise be sensitive if it were linked with individuals. Judicial data regulations should specify categories of information for which these statistics should be made public and proactively disclosed. They should specify the lowest acceptable level or unit of aggregation, such as court complexes, districts, or talukas.

⁵⁶ eCommittee Supreme Court of India. 2016. 'Case Management Through CIS 3.0 (Case Information system 3.0)', E-Courts, p. 204, available at https://ecourts.gov.in/ecourts_home/static/manuals/Case%20Management%20through%20CIS%203.0.pdf

5. Timing of access

In the interest of the fairness of proceedings, the rules of many High Courts specify that copies of documents, including pleadings, depositions, and other parts of the record are typically only made accessible to third parties after the conclusion of proceedings, except in exceptional circumstances where good cause is shown⁵⁷. This principle should be retained in the digital context and incorporated within judicial data regulations.

In other jurisdictions, the stage of a case is accounted for in determining the extent of public access to documents. In the USA, for example, grand jury proceedings are closed to the public and the media both in federal and state courts and grand jury indictments are sealed until after an arrest is made⁵⁸. Following an arrest or indictment, pre-trial service officers investigate defendants' backgrounds to help judges set bail and terms of pre-trial release. Therefore, pre-trial reports are solely directed to the judge and not available to the public. All these rules are designed to protect the integrity of the process and preserve the right to a fair and impartial trial. In the UK, Crown Court judges and magistrates may make pre-trial rulings on the admissibility of evidence, or on points of law relevant to a forthcoming trial, and undertake preparatory hearings in terrorism-related cases and other cases such as long, complex or serious cases, and serious fraud cases. Automatic statutory restrictions prevent the reporting of these rulings⁵⁹. These restrictions continue until the trial has been concluded, when they automatically cease to apply⁶⁰. In some courts in Canada, documents relating

to bail applications (affidavits, reference letters, and conditions of release prepared by the court) are not available to the public before a judge has heard and determined the bail application. Pre-sentence reports are also not available to the public before a judge has imposed sentence⁶¹.

Live streaming of cases has recently begun on a trial basis in some courts, such as the High Courts of Gujarat and Karnataka⁶². For live streaming of cases, the stages for which public interest is arguably most important are final arguments and pronouncement of judgment. These stages are open to the public for all cases not heard in-camera. However, all stages could be live streamed for cases of public importance. In an ideal scenario, court staff will be responsible for censorship of sensitive information through the use of time-delay in the telecast, and the same stage-specific rules would apply. For cases not live-streamed, but for which the recording may be posted online, the court may direct that certain parts should be excluded. Privacy risks associated with live streaming should not deter litigants or lawyers from relying on a given piece of data in support of their claim in court.

⁵⁷ Rule 10, Original Side Rules of the High Court of Calcutta, 1914; Rule 2(ii-iii), Part B, Chapter 5, Vol. 5, Delhi High Court Rules and Orders, Rule 2, Chapter XIII, Rules of the Gauhati High Court, 1954; Rules 212 and 227, Jammu and Kashmir High Court Rules, 1999; Rules 356-358, Civil Court Rules of the High Court of Jharkhand; Rule 148 of the Court Rules of the High Court of Jharkhand; Rules 2-4, Chapter XII, High Court of Manipur Rules, 2019; Rule 2, Chapter XII, Rules of the High Court of Meghalaya, 2013; Rules 356-358 of Civil Court Rules of the High Court of Judicature at Patna; Rule 169, Criminal Court Rules of the High Court of Judicature at Patna;

Rule 3(2-2A) Punjab Civil and Criminal Courts Preparation and Supply of Copies of Records Rules, 1965, Rules 206-208; and the Sikkim Civil Courts Act, 1978

⁵⁸ Administrative Office of the United States Courts. 'A Journalist's guide to the Federal Courts', United States Courts, available online at https://www.uscourts.gov/sites/default/files/journalists_guide_to_the_federal_courts.pdf (accessed on 30 December 2020)

⁵⁹ Section 8C of the Magistrates' Courts Act 1980; Section 41 of the Criminal Procedure and Investigations Act 1996; Section 11 of the Criminal Justice Act 1987; Section 37 of the Criminal Procedure and Investigations Act 1996

⁶⁰ Judicial College. 2014. 'Reporting Restrictions in the Criminal Courts', Courts and Tribunals Judiciary (UK), June, available online at <https://www.judiciary.uk/wp-content/uploads/2014/06/Reporting-Restrictions-Guide-2014-FINAL.pdf> (accessed on 30 December 2020)

⁶¹ Supreme Court of British Columbia. 2011. 'Court Records Access Policy', available at https://www.bccourts.ca/supreme_court/media/BCSC_Court_Record_Access_Policy.pdf (accessed on 30 December 2020)

⁶² High Court of Gujarat. 2020. Order dated 26 October 2020. High Court of Gujarat. Available online at <https://gujarathighcourt.nic.in/hccms/sites/default/files/miscnotifications/Order%20of%20Honourable%20the%20Chief%20Justice%20-%20Experimental%20Live%20Streaming%20of%201st%20Court%20Proceedings.pdf>; Krishnaprasad. 2021. 'Karnataka HC to live stream its proceedings on trial basis', 31 May, The Hindu, available online at <https://www.thehindu.com/news/national/karnataka/karnataka-hc-to-live-stream-its-proceedings-on-trial-basis/article34687757.ece>

6. Obligations

Most data protection regulations identify obligations of data fiduciaries, processors, and other similar roles, to ensure that their use of data does not violate the rights of data principals. These should be strengthened in the judicial context since personal information is already widely available in judicial records, and should remain so, in the interest of open justice. Such obligations are not as important for the use of judicial data by actors in the context of judicial proceedings – litigants, lawyers, courts, and rest of the justice system, because existing laws and rules govern their use of documents. These obligations should mainly be imposed upon actors outside the justice system who access court records and use judicial data it, since existing procedural laws and court rules mostly regulate access to data within the justice system, and between parties in court cases and lack specific instructions on third-party usage outside the justice system.

Some of these obligations should be absolute, as creating exceptions to them would likely offer few benefits, but would create privacy and other risks. These are the following:

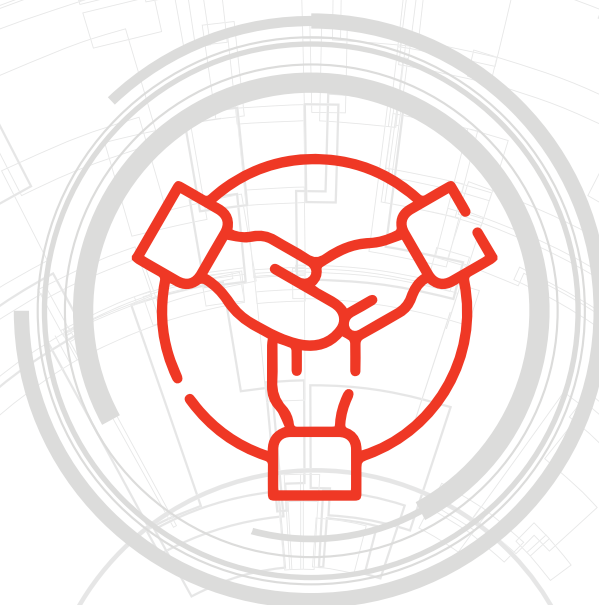
1. Any data fiduciary must process data for a clear, specific, and lawful purpose.
2. They must have a duty to process data in a fair and reasonable manner⁶³.
3. There must be a purpose limitation, in which the data is processed only for a clear, specific, and lawful purpose⁶⁴. In some examples relevant to judicial data discussed below, these should require specific authorisation from whichever authority the judiciary designates as having the power to do so.

In addition, the means of processing must be compatible with the purpose to prevent ‘function creep’⁶⁵.

4. There must be restrictions on the purposes for which data can be used, by fiduciaries both external and internal to the judiciary. These should include profiling, surveillance, and merging judicial data with other datasets for purposes unrelated to adjudication without the knowledge and consent of the principal.
5. Fiduciaries must maintain accurate data and respond to principals’ requests to correct inaccuracies.
6. They must implement security measures to secure the data against misuse or breaches and demonstrate such implementation.
7. They must notify data principals about any breaches, including the nature and type of data on the principal involved in the breach. If external to the judiciary, they must report all breaches to the court or other judicial authority responsible.
8. They must cooperate with the judiciary in audits of all practices relating to judicial data, including collection, storage, processing, dissemination, and other issues related to compliance.

Other obligations would also be retained but would be curtailed significantly in the judicial context. These include the following:

1. The fiduciary must seek and obtain informed consent, freely given and capable of being withdrawn, before processing.
2. They must notify the principal of processing, informing them of the purpose means of processing, nature, volume, and data source.
3. They must provide the principal with access to their data.
4. They must not retain data any longer than the purpose for which it is required.



⁶³ This is a modified version of the provisions in clause 5(a) of the PDP Bill, proposed in Sinha et. al. ‘An Annotated Version of the Personal Data Protection Bill, 2019’

⁶⁴ OECD. 2013. The OECD Privacy Framework, OECD. Available at http://oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (accessed on 2021 05 01)

⁶⁵ Sinha et. al. ‘An Annotated Version of the Personal Data Protection Bill, 2019’

Given that there are significant risks associated with providing access to bulk data, responsibilities that flow from such access should be discussed in detail. Courts should place conditions on such access. These may include mandatory registration by the requestor (data recipient) on the court website or entering into user/confidentiality agreements with the requestor. For example, the Canadian Model Policy for Access to Court Records recommends registered access or access agreement with the court as a precondition for access to bulk records⁶⁶. Monthly limits can be imposed on the volume of records accessed by the requestor. For example, the Volume Service Agreement by the Nebraska Judicial Branch in the USA state that case search activity shall not exceed 20,000 records per month⁶⁷. Bulk access can be restricted to certain kinds of information, and there should be a prohibition of the use of court records to obtain names, addresses or any other information for the purpose of solicitation or sale or for any purpose in which the requestor can reasonably anticipate the receipt of monetary gain from direct or indirect use of such public records. The requestor should be required to use the records according to all laws, regulations, rules, judicial and administrative decisions applicable to it, relevant industry guidelines, and its own privacy policies. Courts should conduct discretionary audits of the data requestor to verify compliance with the terms and conditions. In another example from the USA, one of the conditions of bulk access in Arizona courts is that the data requestor must agree that the data custodian may audit the requestor's compliance with the terms and conditions of the access agreement and that requestor will cooperate fully with any law enforcement investigation concerning the use of the data by the requestor or any of its subscribers⁶⁸.

There should be specific responsibilities for members of the

general public who request and receive bulk data. Data recipients must delete any PD/SPD that is inadvertently included in the information provided to it immediately upon discovery and must disclose both the inclusion and deletion of this information to the data principal, regulatory body and relevant courts. In the event that the data recipient becomes aware of any data breach or a breach of the conditions of access, it must forthwith inform the court which has granted them access to its records and the data principal if the data breach concerns any PD/SPD. They must cooperate with the courts in any audit of the data recipient. They should also cooperate with prosecutorial authorities in any action brought against them relating to the misuse of the information. The data recipient shall indemnify the court, and its officers and employees, from all losses and damages sustained or incurred because of any non-compliance with the conditions of access⁶⁹. For an indication of role-based responsibilities, refer to Annexure 2.

⁶⁶ Section 5.2, Model Policy for Access to Court Records in Canada Judges Technology Advisory Committee Canadian Judicial Council, September 2005, pg.14, available online at https://cjc-ccm.ca/cmslib/general/news_pub_techissues_AccessPolicy_2005_en.pdf (accessed on 30 December 2020)

⁶⁷ Clause 2, Nebraska Judicial Branch Court Case Searches -Volume Service Agreement; available online at https://www.nebraska.gov/subscriber/pdf/JUSTICE_Addendum_One.pdf (accessed on 30 December 2020)

⁶⁸ Arizona Code of Judicial Administration. 'Requests for Bulk or Compiled Data', Clause D.2.d, Section 1-605, Chapter 6- Part 1, Arizona Judicial Branch, available online at https://www.azcourts.gov/Portals/0/admcode/pdfcurrentcode/1-605_Amended_08-2011.pdf (accessed on 30 December 2020)

⁶⁹ For example, one of the clauses in the Bulk Data Access Agreement used by the courts of North Dakota stipulates, "User (data recipient) agrees to defend, indemnify, and hold harmless the North Dakota Supreme Court, the Administrator, its employees, and the State of North Dakota from all loss, risk of loss, and damages sustained or incurred because of or by reason of any claims demands, suits, actions, judgments, or executions for damages of any and every kind and by whomever and whenever made or obtained, allegedly caused by, arising out of, or relating in any manner to any use made of the data or information obtained under this Agreement."

FIGURE 3: OBLIGATIONS OF DATA FIDUCIARIES




7. Rights of data principals in the judicial context

Given that the interest of fair administration of justice can conceivably override privacy concerns in certain situations⁷⁰, PD would be made public, and SPD may also be made public, if determined to be of sufficient public importance (for example, in PILs, cases involving public officials etc). The data principals that this data pertains to should still have a means of redressing any harm that is done to them through the use of this data.

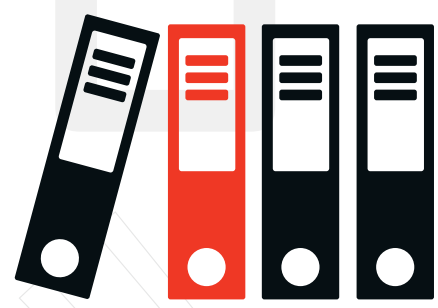
In the non-judicial context, many data protection regulations use rights to achieve this purpose. In the judicial context, however, typical rights such as those relating to erasure and consent would not apply, especially against other parties and lawyers, the court, and other justice system institutions such as police. The principal should still be entitled to the protection of other aspects of their privacy that are not determined purely by access to information, but in the active use of it to harm someone, such as using knowledge of someone's address to follow or harass them⁷¹. Specific data protection rights could help the judiciary ensure that this data, once public, can still be protected from misuse by parties outside the justice system.

Specific data protection rights remain a powerful tool to enforce the more general fundamental right to privacy. Rights-based data protection serves to plug gaps for which consent is an inadequate or inappropriate mechanism⁷². It would therefore be useful to retain the rights themselves. Judges would retain discretion to curtail them in the interest of fair administration of justice. We therefore recommend that the judicial data regulations incorporate a set of data protection rights,



which are suitably modified for the judicial context, and which codify the situations and roles in which there are exceptions to each right in the interest of the administration of justice. These may include:

1. Rights such as the right to confirmation of another party's possession and usage of one's data and the right to access this data;
2. the right to correction;
3. the right to data portability; and
4. the right to be forgotten (for specific contexts)



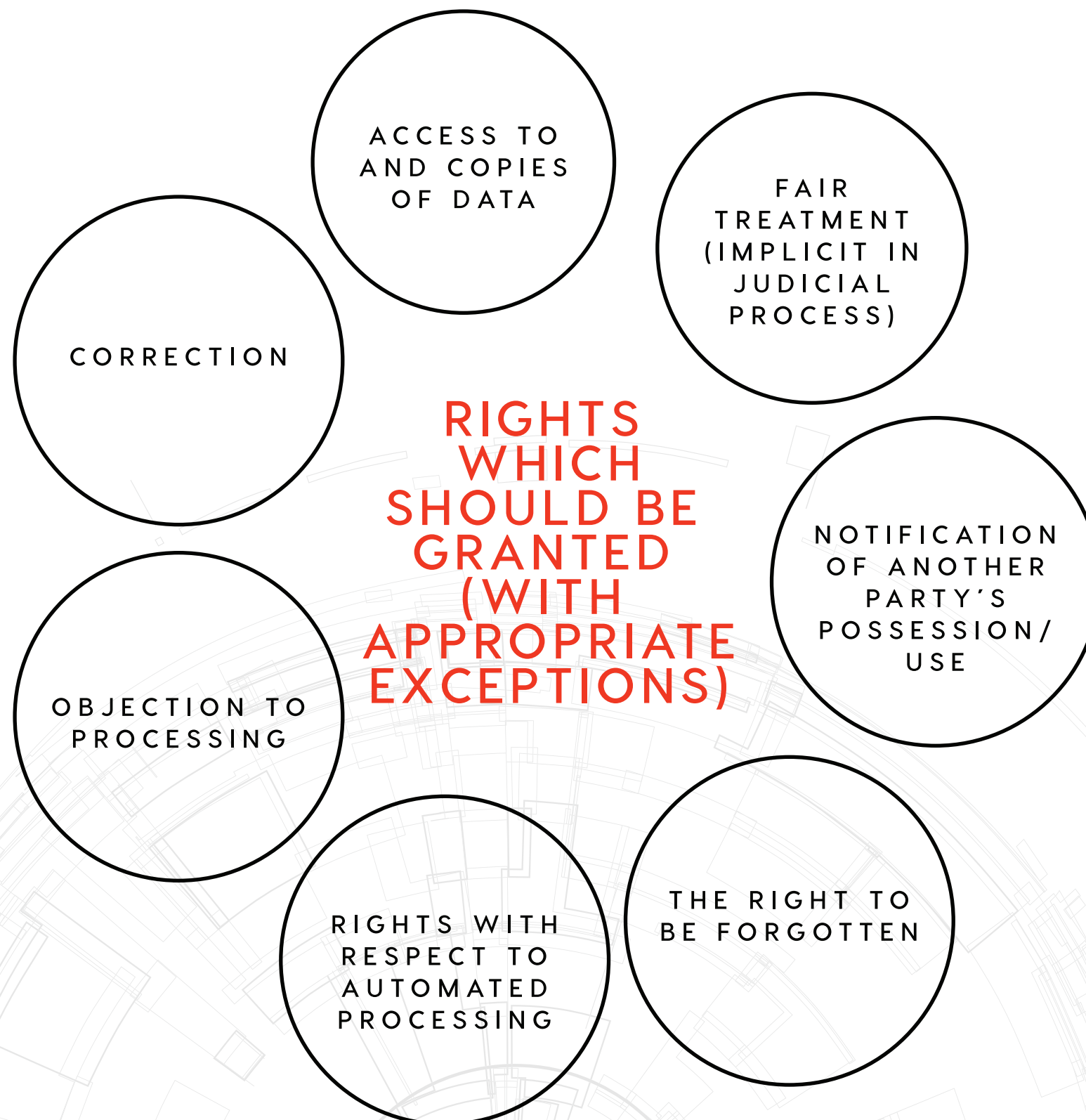
Given that orders and judgments must contain personal information, some rights may prove to be very important, such as rights in respect to automated processing, in which the principal is granted a right not to be the subject of an automated decision. There are numerous concerns regarding the use of advanced algorithms in judicial applications, which raise complex ethical and legal questions regarding the due process of law. As such, rights with respect to automated processing are necessary for the use of judicial data. Unlike other rights, which are often exempted from application to legal proceedings, this right must be strengthened in the judicial use of data to preserve the fairness of the judicial process. A right to fair treatment is taken to be implicit in the context of judicial proceedings through the application of the doctrine of due process and other constitutional values. However, it serves a valuable purpose with respect to third party processing of judicial records. This right should explicitly include rights against surveillance by state agencies, including those within the justice system and discrimination based on social and economic divisions such as caste, religion, and gender.

⁷⁰ R. Rajagopal v. State of Tamil Nadu, 1994 SCC (6) 632, discussed in greater detail in Paper I: Balancing Open Courts with the Right to Privacy – The Indian Perspective

⁷¹ For example, see Daniel J. Solove... 'A Taxonomy of Privacy', on 'intrusion' as a form of privacy harm.

⁷² Rahul Matthan. 2017. 'Beyond Consent – A New Paradigm for Data Protection', Takshashila Discussion Document, 2017-03.

FIGURE 4: RIGHTS OF DATA PRINCIPALS



C. BUILDING INSTITUTIONAL CAPACITY FOR THE REGULATION OF JUDICIAL DATA

1. Scope of application of PDP Bill to the judiciary

Section 2 of the PDP Bill states that the Bill is applicable to the processing of personal data by the Indian government, any Indian company, citizen, or person/body of persons incorporated or created under Indian law.

The framework of the Indian judicial system has been laid down by the Constitution of India, and the judicial system derives its powers from it. The Supreme Court of India and the High Courts in various states have been constituted under the Indian Constitution⁷³. The subordinate courts are established under the Code of Civil Procedure, the Code of Criminal procedure and several erstwhile British-era legislations which have been adopted into the laws of independent India⁷⁴. Several tribunals and other subject- matter specific courts have also been established under specific legislations. Further, Section 19 of the Indian Penal Code defines a “Judge” as “...who is one of a body of persons, which body of persons is empowered by law to give a judgment.” Hence, all the courts and tribunals constituted under any laws in force in India are brought within the scope of application of the PDP Bill.

Section 36(c) of the PDP Bill specifically exempts the processing of personal data by any court or tribunal in India in exercise of any ‘judicial function’ from its scope of application. In such situations, the data protection

obligations of consent, notice, data principal rights and accuracy will not apply. However, the general obligations with regard to security safeguards (Section 24) and fair and reasonable processing (Section 4) will continue to apply even when judicial functions are carried out. Courts and tribunals conduct a variety of non-judicial, administrative tasks for their proper functioning. The exemption in Section 36(c), therefore, will not cover a situation where the courts or tribunal are processing personal data in exercise of such non-judicial functions. These will be governed by the provisions of the PDP Bill.

Unlike the GDPR which specifically stipulates that the supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity⁷⁵ and envisages entrusting supervision in such situations to specific bodies within the judicial system of the member states, there is no parallel provision in the PDP Bill. The jurisdiction of the Data Protection Authority of India (“DPAI”) to be established under the PDP Bill extends to all data fiduciaries and data processors to whom the provisions of the PDP Bill are applicable. This would mean that in so far as the courts and tribunals are processing data in the exercise of judicial functions, the DPAI will have no competence over such processing. However, when the courts and tribunals are processing data for non-judicial functions, the DPAI would have competence over such processing. However, when the courts

and tribunals are processing data for non-judicial functions, the DPAI would have competence over such processing as in such situations the courts and tribunals are acting in the capacity of data fiduciaries and data processors covered under the purview of the PDP Bill.

Therefore, it is clear that the Parliament recognizes that preserving judicial independence is a must when judicial functions are carried out and the provisions of the PDP Bill are inappropriate for application in the context of judicial functions.

⁷³ Article 124 and 216 of the Constitution of India

⁷⁴ Article 236 and 237 of the Constitution of India

⁷⁵ Article 55 of the GDPR

2. Regulatory autonomy for judicial functions

The separation of powers between the legislature, executive, and judiciary is a fundamental tenet of Indian democracy. Following from this principle and the need to maintain judicial independence, the institutional framework governing judicial data must empower the judiciary to independently make decisions governing judicial data.

A body that regulates judicial data should thus have a majority representation from the judiciary. Further, it should not consist of sitting judges to avoid conflicts of interest. The body should consist of retired judges and technical experts in privacy and digital security. Such a body will have jurisdiction over the processing of data in the exercise of judicial functions by the courts and the use of judicial data by third parties. The roles and responsibilities should be structured in a way that ensures that the functional specialisation of individuals in it is maximised, while not exhausting their time and effort in handling challenges outside of their core competencies. While the retired judges will bring in judicial expertise the experts in privacy and digital security will fill in gaps in technical areas where the judiciary lacks expertise.

The level of institutional and regulatory capacity needed will depend on the extent of development of ICT in the Indian judiciary. At the present level of maturity, the chief responsibilities of the body would include formulating and drafting model privacy policies and access policies for the various sources of judicial data. These would be designed for the E-Courts portal, the NJDG, several mobile applications used by the

judiciary, and for the websites of High Courts and the Supreme Court, which they may adopt and ratify with or without modification. This body could also support and advise the eCommittee of the Supreme Court of India with regard to designing future information systems to allow open access to judicial records while following privacy-by-design. It could assist in training judges and court staff regarding the technical aspects of privacy in order to increase awareness of the associated risks. Conducting research and consulting experts in fields ranging from privacy law to information security would result in a policy that can mitigate emerging risks and challenges. In this early stage, the responsibility for grievance redressal regarding illegal and irregular data processing can remain with courts themselves, with the privacy policy specifying the process and protocol to be followed in handling such cases.

Phase III of E-Courts proceeds to make radical changes to the nature and volume of information that will be made accessible. Since this process will require considerable amendments to various laws and rules, the body should be tasked with determining what legal changes, both procedural and substantive, would be necessary to ensure that these documents can be safely made public.

Working towards open standards for information generated by judicial processes would be an important part of facilitating open justice through the design of information systems. With further advances in court information systems development in India, the body could test the standards and policies that it drafts on a pilot basis by creating an open database, with a

limited set of data, open for the public and other actors to use, subject to restrictions imposed to preserve privacy and in line with the privacy policy of such a database.

When ICT in the Indian judiciary reaches a high level of maturity and judicial processes are almost entirely digitised, and when data fields are marked up in judicial documents, the regulatory capacity required will be much greater. This would especially be the case if API access to judicial data is granted and third parties are then able to access large volumes of data quickly. At that time, a single body may not have the flexibility to adapt to the jurisdictional variations across High Courts while having the capacity to regulate the volume of data that would be available at this stage. Therefore, there are two alternate structures that may potentially be adopted:

- The regulatory body will be a voluntary association consisting of retired judges from the Supreme Court and High Courts. This body can have benches across India to allow for people in diverse geographies to access it. This structure enables the High Courts to maintain their independence, since they have a choice to be a part of this body. At the same time, it will create uniformity of practice and precedent across the country that will enable better compliance. The disadvantage of this system is that High Courts will not be able to develop their own procedures for regulating judicial data.

- The Supreme Court and each high court will have their own regulatory bodies. The advantage of this structure is that it allows High Courts to maintain their autonomy

vis-à-vis regulating judicial data. The disadvantage with this structure is that it allows for the creation of a confusing regulatory framework that will vary from state to state. This makes compliance difficult. Enforcement of orders beyond state boundaries may also become complicated.

Regarding the functions of these regulatory bodies, they shall:

- Be responsible for redressal of grievances arising out of processing, access or use of judicial data.
- Establish security standards and data handling protocols governing judicial data.
- Arrange periodic training for judges and court staff on the framework for privacy in judicial data and their role and responsibilities within this framework.
- Arrange for periodic audits of third parties to ensure compliance with the framework.
- Liaise with the general data protection regulator in the country (as envisaged under the PDP Bill) to keep abreast of the latest developments in the field.

⁵¹ National Criminal Justice Association. 'Justice Information Privacy Guideline – Developing, Drafting and Assessing Privacy Policy for Justice Information Systems'

⁵² National Criminal Justice Association. 'Justice Information Privacy Guideline – Developing, Drafting and Assessing Privacy Policy for Justice Information Systems', p.64.

D. RECOMMENDATIONS

1. Appoint a dedicated body to formulate privacy regulations for the judiciary

The judiciary needs to appoint the regulatory body described above. At this early stage, its key responsibilities would be to:

(a) Review the current arrangements and provisions for accessing court records across different courts in India. The various different jurisdictions in the judicial system makes it complex to do anything that cuts across the entire regime, with each jurisdiction subject to its own procedural rules and treatment of court records and judicial information. Therefore, each jurisdiction warrants individual attention in any proposals.

(b) Conduct research on emerging privacy risks that would result from the improved public dissemination of judicial data that has been made possible by technological advancements.

It should then use this research and the public discourse described below to develop an access, privacy and data protection framework for the judiciary that can achieve the appropriate balance between judicial transparency and privacy.

2. Consult and involve stakeholders in the policy formulation process.

Creating a data protection framework for the judiciary requires thorough discussion on how existing policies

that make sense for physical courtrooms would be inappropriate if simply replicated in a digital world. The data protection framework for a digitalised judiciary must be tailored to each stakeholder of the judicial system based on their specific needs, rights, and obligations, both as a data subject as well as user of judicial data.

The expert body should hold consultations among the general public and relevant stakeholders (including court users) to solicit their views and experience of the practical administration of open justice in modern society. It should also seek their opinion on the application of rights relating to equality, confidentiality, privacy (including but not limited to data protection), fair trial and offender rehabilitation in the context of public access to judicial data. As it drafts and revises the policy, the expert group should solicit views and publish responses from a diverse and inclusive set of stakeholder groups.

3. Map information flow and classifying data elements

One of the most crucial steps in drafting a privacy policy is analysing the data elements (i.e., pieces of information) in a judicial proceeding. Such an analysis, in turn, involves mapping information flow, determining attributes of data elements (e.g., nature or sensitivity of the information that is being disclosed), and then establishing a privacy baseline or presumption⁷⁶. Pursuant to the open courts principle, the preferred position would be the presumption of public access to court records. The courts may then formulate rules/guidelines to depart from the default position for

⁷⁶ Global Justice Information Sharing Initiative. 2007. Privacy and Civil Liberties Policy Development Guide and Implementation Templates. Washington D.C.: United States Department of Justice. Available online at https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/Privacy_Guide_Final_0.pdf (accessed on 02 June 2021)

⁵² National Criminal Justice Association. 'Justice Information Privacy Guideline – Developing, Drafting and Assessing Privacy Policy for Justice Information Systems', p.64.

preserving individual privacy and public safety. This mapping process helps to understand the role of data in the judicial process, and therefore, its role in ensuring transparency of this process. It is also necessary to understand the risks to both privacy and fair administration of justice that would result from disclosure to various groups, from the general public to the media.

4. Draft a model privacy and access policy

Develop an access model, with appropriate restriction mechanisms, that delivers effective access to court records and other judicial data. The model should clearly identify the scope and objective of the policy, determine how information is verified, maintained and corrected, decide who gets access, what information can be accessed by whom and determine the method of access (physical/remote) and conditions on access (restrictions on use, inspections, user contracts). While devising the model policy, a key part of the process will be to identify existing laws, rules, policies, and practices that will need to be amended to prevent conflict with the model policy, for example, streamlining RTI rules for accessing court records. The extent of a user's access to judicial data should be determined by considering the rights of data subjects and imposing obligations on users of such data. These rights may be either curtailed or enhanced based on other contextual factors. These factors could include the stage of a case (timing of access), the sensitivity and granularity of the data, the public interest in the disclosure of that data, and the subject matter or case type.

5. Implement 'privacy-by-design in the development of information systems for the judiciary

Courts need to address privacy issues during the planning stages of their information systems. By addressing privacy at the planning stages, the resulting technology has the best chance of providing desired privacy protections. As Phase III of the E-Courts project approaches, there are great opportunities to make data more accessible for citizens and organisations to utilise⁷⁷. In addition, private sector expertise could help in the development of advanced information systems for the judiciary⁷⁸. However, this implementation without privacy planning can result unintended harms and having to retool the system to address these effects⁷⁹. The problem compounds when the system itself has difficulty authenticating or correcting information, and in fact has the contrary effect of legitimising and perpetuating incorrect information. This requires communication of a clear vision and core values of judicial system to the technology implementers at the outset of the information system's initiative.

⁷⁷ DAKSH, Whitepaper Series on Next Generation Judicial Platform, Paper 3: Legal Framework.

⁷⁸ DAKSH. 2019. Whitepaper Series on Next Generation Judicial Platform, Paper 2: Transition and Implementation. DAKSH: Bengaluru, available online at https://dakshindia.org/wp-content/uploads/2020/02/Paper-2_Transition-and-Implementation.pdf (accessed on 30 December 2020)

⁷⁹ DAKSH, Whitepaper Series on Next Generation Judicial Platform, Paper 3: Legal Framework.

FIGURE 5: RECOMMENDATIONS;



TABLE ILLUSTRATING ACCESS REGULATIONS BASED ON ROLE, GRANULARITY AND VOLUME OF DATA

	CASE-BY-CASE	BULK RAW DATA
LITIGANTS	Full access to information from their own case except when restricted by law or restricted/sealed by the courts	Same as the general public
LAWYERS/ADVOCATES	The same level of access as their client	Same as the general public
WITNESSES	Generally, same as the general public; additional information such as evidence, affidavits, police reports, if court deems it necessary for accurate testimony/opinion.	Same as the general public
INVESTIGATION AGENCIES/ LAW ENFORCEMENT/ COURT-APPOINTED OFFICERS	Complete access in the context of specific cases, in which they have jurisdiction	Same as the general public
PRISON OFFICIALS	Partial or complete access with court's permission if necessary for safety and well-being of prisoners	Same as the general public

TABLE 3: WHICH DATA SHOULD BE PROVIDED ON A CASES-BY-CASE BASIS, AND WHICH DATA CAN BE PROVIDED IN BULK

	CASE-BY-CASE	BULK RAW DATA
GENERAL PUBLIC	All open data including judgments, orders, and cause lists. If these documents contain SPD, it should be redacted/anonymised unless the court determines that public interest outweighs privacy	Bulk records of open data- E-Courts (PD/SPD redacted)
JUDGES EXERCISING JUDICIAL FUNCTIONS	Full unrestricted access	Full unrestricted access
JUDGES EXERCISING ADMINISTRATIVE FUNCTIONS	Generally, only public version of records unless full access is necessary for the supervision of the judge who decided the case	Full access to records under the jurisdiction for inspection, performance evaluation, reforms
REGISTRY STAFF	Judicial wing – full access within the jurisdiction, administrative wing – only if necessary/ relevant to functions	Access within same conditions as case-by-case access
COURT CLERK	Same as the judge whose courtroom they are serving	Same as the judge whose courtroom they are serving
MEDIA AND JOURNALISTS	Same as the general public	Same as the general public

TABLE 3: WHICH DATA SHOULD BE PROVIDED ON A CASES-BY-CASE BASIS, AND WHICH DATA CAN BE PROVIDED IN BULK

	CASE-BY-CASE	BULK RAW DATA
GENERAL PUBLIC	All open data including judgments, orders, and cause lists. If these documents contain SPD, it should be redacted/anonymised unless the court determines that public interest outweighs privacy	Bulk records of open data- E-Courts (PD/SPD redacted)
JUDGES EXERCISING JUDICIAL FUNCTIONS	Full unrestricted access	Full unrestricted access
JUDGES EXERCISING ADMINISTRATIVE FUNCTIONS	Generally, only public version of records unless full access is necessary for the supervision of the judge who decided the case	Full access to records under the jurisdiction for inspection, performance evaluation, reforms
REGISTRY STAFF	Judicial wing – full access within the jurisdiction, administrative wing – only if necessary/ relevant to functions	Access within same conditions as case-by-case access
COURT CLERK	Same as the judge whose courtroom they are serving	Same as the judge whose courtroom they are serving
MEDIA AND JOURNALISTS	Same as the general public	Same as the general public
ACADEMIA/ RESEARCHERS	Generally, only open data. On showing sufficient cause, access to affidavits, witness or expert testimony or other evidence, police reports etc., as such information may be required for studying the practical effect of certain laws.	Same as the general public

TABLE 3: WHICH DATA SHOULD BE PROVIDED ON A CASES-BY-CASE BASIS, AND WHICH DATA CAN BE PROVIDED IN BULK

	CASE-BY-CASE	BULK RAW DATA
CONTRACTORS/ VENDORS APPOINTED BY THE COURT	Generally, only open data, unless courts/eCommittees/other authorities under judiciary authorise greater access to carry out the delegated task	Access within same conditions as case-by-case access
EXTERNAL LAW-TECH ENTITIES	Generally, only open court records. However, access to other court records may be granted on showing sufficient cause for a very limited set of applications set out in codified regulations and subject to certification, approval, close monitoring, and auditing by the body.	Access within same conditions as case-by-case access
LEGAL AID ORGANISATIONS	Open data generally, full access to specific cases if court designates them or a party requests them, with party's consent	Same as the general public

TABLE OF POTENTIAL DATA-RELATED RESPONSIBILITIES ASSOCIATED WITH EACH ROLE IN THE CONTEXT OF JUDICIAL PROCEEDINGS

LITIGANTS	Parties should not volunteer PD/SPD about themselves or if not necessary to defend themselves/their claim effectively.
LAWYERS/ADVOCATES	They must maintain adequate safeguards of all PD/SPD
WITNESSES	They must sign an undertaking not to use or disclose any PD/SPD they may have access due to their participation in the case.
INVESTIGATION AGENCIES/ LAW ENFORCEMENT/ COURT-APPOINTED OFFICERS	Investigation agency/ law enforcement/ court appointed officers must not disclose or use for any purpose, any PD/SPD they have access to due to participation in a case.
PRISON OFFICIALS	Judicial data containing PD/SPD held by prisons with the court's permission must not be used for any purpose other than their mandate and must not be disclosed. If the government/ law enforcement or investigation agencies request access, prison officers should redirect requests to court.

TABLE 4: RESPONSIBILITIES ASSOCIATED WITH EACH ROLE

TABLE 4: RESPONSIBILITIES ASSOCIATED WITH EACH ROLE

GENERAL PUBLIC	Must comply with all conditions of bulk access, current laws, rules and policies governing the judicial data and information, privacy, and confidentiality of the data and information provided to it
JUDGES EXERCISING JUDICIAL FUNCTIONS	While writing judgements, the judge should omit PD/SPD unless relevant for understanding the reasoning for the decision. They should tag all PD/SPD in the judgment for redaction/ anonymisation before granting access to records. When requests are made to the bench seeking PD/SPD about the participants not mandated to be disclosed under the law, the judge must assess relevance to the decision before deciding whether or not to grant access.
REGISTRY STAFF	They must only access information relevant to carrying out functions entrusted to their sections. They must ensure robust security safeguards are maintained and necessary steps to prevent misuse, unauthorised access to, modification, disclosure or destruction of personal data; these should be reviewed periodically. They should be responsible for de-identifying personal and SPD before access to court records is granted, including information tagged as PD/SPD by the judge. If the Registry believes that there are additional PD/SPD, they should bring such information to the judge's notice and act according to his instructions.
COURT CLERK	They should use the PD/SPD they have access to only to assist the judge in carrying out his functions. They should handle the records in the courtroom with extreme care and caution and ensure that such records can be viewed only by the judge.
MEDIA AND JOURNALISTS	The media should provide bonafide contact information and accreditation information, as is necessary to verify their credentials. They should destroy physical and electronic data supplied within a specified time period (although details of individual cases for journalistic purposes can be retained longer with the court's permission). The media should not deny third parties access to this data, even if these third parties seek to use this data for non-journalistic purposes. It must strictly comply with reporting restrictions and any other legal restrictions on the use of this data.

TABLE 4: RESPONSIBILITIES ASSOCIATED WITH EACH ROLE

ACADEMIA/ RESEARCHERS	<p>Researchers must provide evidence to the courts regarding the purpose and intended outputs of their research, how it will benefit the public, how the request for data is specifically, explicitly and legitimately required for the project purpose, how PD/SPD will be kept secure throughout the project duration. The researcher shall indemnify the court from harm resulting from the violation of conditions of access.</p>
CONTRACTORS/ VENDORS APPOINTED BY THE COURT	<p>The contractor must enter into a confidentiality agreement with the judiciary, prohibiting the use or dissemination of data for any purpose other than the services it provides the judiciary. They must give the court a detailed description of the product/service and why access to PD/SPD is required. It must cooperate with the courts/ E-committee in audits of compliance with conditions of access and should promptly respond to their questions and queries. The contractor shall indemnify the Court from all harm resulting from the violation of conditions of access.</p>
EXTERNAL LAW-TECH ENTITIES	<p>The recipient must provide evidence to the courts on how the request for data is specifically, explicitly the and legitimately needed to develop services or products that contribute towards increasing access to justice or facilitating the administration of justice. They must provide proof of mandated security measures, compliance with conditions of access and all laws, rules and policies governing data and information, privacy, and the confidentiality of the data and information provided to it. They must cooperate with courts during audits of their data use. They must indemnify the court from harm resulting from the violation of the conditions of access. Some of the purposes for which they process data should entail specific obligations, such as seeking and obtaining the consent of parties and others whose information is contained in these records.</p>
LEGAL AID ORGANISATIONS	<p>Legal aid organisations must provide evidence to the courts on how data they request is specifically, explicitly and legitimately required to provide legal aid services; they must provide evidence of adequate security measures, they must undertake that further processing of the data/information obtained by it will only be used for the lawful purpose of providing legal aid services. The legal aid organisation must inform and educate data principals whose PD/SPD data they possess of their privacy and data protection rights and obtain their consent to the processing, wherever appropriate. It must also undertake to comply with all conditions of access and with all laws, rules, and policies governing disseminating data and information and privacy. It must cooperate with the court's audits. The organisation shall indemnify the court from harm resulting from the violation of conditions of access.</p>

TABLE OF POTENTIAL RESPONSIBILITIES OF COURTS IN RELATION TO OTHER ROLES

LITIGANTS	The courts should determine the relevance of the SPD sought by the party (except when it pertains to the party or opposing party) to the present matter before granting/denying access, and decide on applications to publish or redact SPD from the public record.
LAWYERS/ADVOCATES	Lawyers/advocates should be given sufficient opportunities to tag PD and SPD in filings, transcripts, public documents, e.g., Judgments and orders, and audio-visual recordings of proceedings. The Registry will be responsible for reviewing such requests.
WITNESSES	The court must not disclose PD/SPD pertaining to them unless parties need it to defend themselves/ their claim effectively (e.g., for cross-examination), it is necessary for the official mandate (e.g., police investigation), or if public interest merits that it is made public for the citizens to understand reasoning the decision
INVESTIGATION AGENCIES/ LAW ENFORCEMENT/ COURT-APPOINTED OFFICERS	Courts may permit these agencies/ officers to retain and use PD/SPD the court has provided access to if necessary for maintaining public order, safety and national security
GENERAL PUBLIC	The judiciary should proactively disclose statistics. Bulk records should only be made available as per specific conditions – refer to the earlier section on bulk data.
JUDGES EXERCISING JUDICIAL FUNCTIONS	The Registry should ensure that the judge has all information about cases in their docket and should ensure that all PD/SPD is appropriately tagged.

TABLE 5: RESPONSIBILITIES OF COURTS IN RELATION TO OTHER ROLES

COURT CLERK	The Registry should ensure that the court clerk is given access to information only in cases that are being adjudicated by the judge they are serving. For cases beyond jurisdiction, the court clerks should be given access to PD/SPD only to the extent granted to the judge they are serving.
MEDIA AND JOURNALISTS	The court should verify the accreditation of professionals and organisations and proactively provide them with information after this. The court should refuse disclosure if it would cause an undue threat to privacy, due process, or law and order. A dedicated media liaison officer should be appointed to respond to queries and restrict reporting when mandated by statute or a court order. Courts should also publish such restrictions on their websites.
CONTRACTORS/ VENDORS APPOINTED BY THE COURT	Before the courts employ a contractor who would require access to judicial data, (including PD/SPD), they must verify that contractor has implemented necessary security measures. The service contract must place stringent conditions on the volume, duration, confidentiality, and uses of data. The courts should monitor and regularly audit the contractor to verify compliance.
EXTERNAL LAW-TECH ENTITIES	The court should place stringent conditions prohibiting the use of court records for any purposes other than the development of the product/service and setting strict timelines for development beyond which access will be revoked. It must perform audits of the requestor/user to verify compliance.
LEGAL AID ORGANISATIONS	Courts should provide bulk access only to registered legal aid organisations. Courts can limit the volume, duration, and kind of information to which access is granted depending on the material provided by the organisation on how it proposes to use the information to provide appropriate legal aid services. The court may, at its discretion, perform audits of the organisation to verify compliance with the terms and conditions of access