Law Enforcement Access to Data in India: Considering the Past, Present, and Future of Section 91 of the Code of Criminal Procedure, 1973

*Tarun Krishnakumar**

Abstract *Developments in modern technology and the Internet have resulted in vastly greater quantities of information being stored in electronic form. In addition to gains for convenience, innovation, and the economy, this trend also means that law enforcement and other government agencies are required to increasingly turn to the digital domain to gather evidence for investigative or enforcement purposes. In the Indian context, this usually means having to rely on pre-digital era procedural powers such as Section 91 the Code of Criminal Procedure, 1973. Drawing from existing literature, case law, and developments in policy, this article seeks to conduct an analysis of Section 91 with a view towards adding to the discourse surrounding calls for its reform. It concludes that, in its current form, the provision neither adequately accounts for privacy concerns nor provides clear and certain procedures for law enforcement agencies to compel production of evidence stored in electronic form. Several principles which have developed around the provision are no longer relevant in the digital age, others have the potential to excessively invade privacy, while several others internally conflict. It would be in the interests of both individuals and law enforcement agencies to seek timely review and reform of this provision to account for modern realities.*

* Tarun Krishnakumar is a lawyer admitted to practice law in India and the United States (California). He is a graduate of the National Law School of India, Bangalore. All views expressed are personal. The developments surveyed in this article are current as of June 2019.

I. Introduction

The proliferation of the Internet, smartphones, and other digital devices has meant that an increasing amount of information – including information considered private[1] – is found in electronic form. Trends in digitisation, automation, computing, and the emergence of data-centric revenue models mean that vastly more quantities and entirely new categories of information are being generated, collected, and processed; previously transient datapoints are being stored more permanently; and there is increasing convergence of services which involve data collection. All this means that, in today's world, it is exceedingly difficult to not leave a digital footprint in ordinary course.[2]

While having positive implications for innovation, commerce, governance, and convenience, these developments also mean that an increasing amount of information relevant for law enforcement and investigative purposes is found in electronic form.[3] Alongside the availability of vastly more types and quantities of evidence for use for investigative purposes by law enforcement agencies ('**LEA**'), this data 'revolution' also raises novel questions from the points of view of personal privacy, due process, and civil liberties.[4] In several jurisdictions, this duality has triggered vigorous debates surrounding the legal standards for LEA[5] to compel production of data stored by individuals or the ubiquitous intermediaries[6] (and service providers) that process and store data on their behalves. Often these debates centre around the procedural safeguards which apply to the ability of LEA to compel production – including issues such as evidentiary standards, proportionality of production

---

1 In this context, 'private' information may be understood to include information that is personal as well as other kinds of information that is considered sensitive including trade secrets and confidential commercial information.

2 *See generally*, Bernard Marr, 'How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read' (*Forbes*, 21 May 2018), <https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#52cd124260ba> accessed 19 October 2019.

3 For a balanced discussion, *see*, Matt Olsen and others, 'Don't Panic: Making Progress in the 'Going Dark' Debate' (Berk*man Center for Internet and Society*, 1 February 2016) 12 <https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf> accessed 19 October 2019.

4 Olsen and others (n 3) 1.

5 For the purposes of this paper, LEA refers to police and other regulatory/enforcement agencies regulated by statute. It does not include intelligence agencies which – in India – are not created by or governed under statute.

6 For the purposes of Indian law, intermediaries are defined by s 2(*w*) of the Information Technology Act in the following terms: "'*Intermediary' with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes*".

orders, protections against self-incrimination, and the need for judicial oversight or authorisation.[7]

While several stakeholders in India have expressed concerns relating to the inadequacy of the procedural framework governing LEA access to data, the debate has been fragmented. Although significant discussion has taken place surrounding a legal framework for privacy and data protection in India,[8] there is scope for deeper examination of LEA powers under Indian criminal procedure law. Where discussions have taken place on this issue, they have largely been at the policy-level and have not deeply engaged with historical trends in caselaw or applicable legal doctrine.

Against this backdrop, this paper aims to contribute to the discourse around these issues by engaging in a legal survey of powers available to LEA under Section 91 of the Code of Criminal Procedure, 1973 ('**Cr.PC**' or '**1973 Code**') – a provision commonly used to compel production of data.[9] In addition to surveying existing research and judicial precedent, this paper attempts to draw from these principles and several related domestic and international developments – to highlight why it is timely to begin considering reforms to this provision and the mechanism under it.

II. Statutory Framework

The Indian legal regime for LEA access to data comprises a patchwork of procedural provisions from frameworks including general criminal procedure law,[10] special criminal law,[11] sectoral

---

[7] For example, in the Indian context, *see*, Rishab Bailey and others, 'Use of Personal Data by Intelligence and Law Enforcement Agencies' (2018) National Institute for Public Finance and Policy Working Paper <http://macrofinance.nipfp.org.in/PDF/BBPR2018-Use-of-personal-data.pdf> accessed 19 October 2019; *See also*, Rahul Matthan, 'The Government and Big Tech Need to Meet Halfway" (*LiveMint*, 11 June 2019) <https://www.*LiveMint*.com/opinion/columns/opinion-the-government-and-big-tech-need-to-meet-halfway-1560247166819.html> accessed 19 October 2019.

[8] Most recently, these debates have centred around the Personal Data Protection Bill 2019 which is soon to be enacted by the Government of India.

[9] For example, *see*, Sahil Makkar, 'Are Private Detectives Prying on Personal Details?' (*Rediff.com*, 18 November 2013) <https://www.rediff.com/news/report/are-private-detectives-prying-on-personal-details/20131118.htm> accessed 19 October 2019; Dheeraj Fartode, 'Now, RPF can monitor Call Data Records for Probe' (*TheHitavada*, 28 April 2016) <https://www.nagpurrailwaypolice.gov.in/sites/default/files/5_11.pdf> accessed 19 October 2019.

[10] As mainly contained in the Code of Criminal Procedure 1973 (CrPC).

[11] For example, the Narcotics Drugs and Psychotropic Substances Act 1985 (NDPS Act) contains specialised procedures for search and seizure. However, where not inconsistent with provisions of the NDPS Act, provisions of the CrPC governing search and seizure will continue to apply (NDPS Act, s 51).

regulations,[12] and information technology law.[13] The framework applicable to a particular case depends on the criminal conduct that is at issue and the authority empowered to investigate it. It important to note that, in most cases, there are no specific carve-outs for access to evidence stored in digital form.[14] Powers relating to *physical* search and seizure – intended to apply to tangible objects and documents at the time of enactment – are applied in relation to electronic evidence.

Within this patchwork, this paper focuses on certain key provisions contained within the general criminal procedural framework, the Cr.PC. The reason for this scoping is two-fold. *First*, Cr.PC powers are most commonly used to compel production as they apply to the widest variety of criminal offences and are available to the widest number of authorities including police and specialised LEA. *Second*, many sectoral or special frameworks, rather than creating specialised procedures, tend to incorporate – by direct reference – provisions of the Cr.PC insofar as summons, search and seizure are concerned. While other frameworks may also provide mechanisms for LEA to access data, these provisions are not as commonly resorted to, usable only in narrowly defined circumstances (or in relation to specific offences), have onerous authorisation requirements on paper, or are available only to a small sub-set of LEA or other government authorities.[15]

Of particular relevance within the Cr.PC are provisions of Chapter VII which relate to "*Processes to Compel the Production of Things*". This Chapter is divided into two sub-chapters: "*Summons to Produce*" and – and where such summons is insufficient – "*Search Warrants*". Sections 91 and 92 pertain to summons, while Sections 93 to 98 pertain to search warrants. Sections 99 – 101 contain general guidance in relation to the manner in

---

[12] *See*, examples cited in Sunil Abraham and Elonnai Hickok, 'Government Access to Private-Sector Data in India' (2012) 2(4) International Data Protection Law 304 <https://doi.org/10.1093/idpl/ips028> accessed 19 October 2019.

[13] As mainly contained in the Information Technology Act 2000 (IT Act) as amended.

[14] A notable exception to this statement is the Income Tax Act 1961 which in its provisions governing search and seizure expressly applies to "*books of account or other documents maintained in the form of electronic record*" [Income Tax Act 1961, s 132(1)(*ii*)(*b*)]. Another example is the Information Technology Act 2000 – which principally applies to regulate conduct in the cyber domain.

[15] For example, s 69 of the IT Act authorises interception, monitoring, and decryption of any information *passing through any* computer resource in relation to a wide variety of matters. However, such powers are only exercisable upon issuance of orders by the Secretary of Home Affairs (Central Government) or the Secretary of the Home Department (State Government) to (currently ten) *agencies designated under the provision*. Only in very limited circumstances can very senior LEA officers themselves order interception under this provision. In this regard, *see*, the Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009. Similarly, s 69B authorises monitoring and collection of traffic data only for cyber security linked purposes.

which searches are to be conducted. This paper will focus on Section 91 (and, to a lesser extent, Section 92) as it has been – and is likely to continue to be – the key focus of debates on LEA access to data. This is because the powers under these provisions, widely exercisable by most LEA around the country, are outdated in as much as they only apply to *physical* objects and also because Section 91 authorises LEA to *unilaterally* compel production – without the need for judicial authorisation or adversarial process.[16] To illustrate, they are extracted below (emphasis supplied):

> *91. Summons to produce document or other thing.—*
>
> (1) Whenever any Court or *any officer in charge of a police station* considers that the production of *any document or other thing is necessary or desirable for the purposes of any investigation*, inquiry, trial or other proceeding under this Code by or before such Court or officer, such Court may issue a summons, or *such officer a written order*, to the person in whose possession or power such document or thing is believed to be, requiring him to attend and produce it, or to produce it, at the time and place stated in the summons or order.
>
> (2) Any person required under this section merely to produce a document or other thing shall be deemed to have complied with the requisition if he causes such document or thing to be produced instead of attending personally to produce the same.
>
> (3) Nothing in this section shall be deemed—
>
> (a) to affect sections 123 and 124 of the Indian Evidence Act, 1872 (1 of 1872), or the Bankers' Books Evidence Act, 1891 (13 of 1891), or
>
> (b) to apply to a letter, postcard, telegram or other document or any parcel or thing in the custody of the postal or telegraph authority.

Section 92 addresses the procedure for seizure and detention of letters and telegrams in transit:

> *92. Procedure as to letters and telegrams.—*
>
> (1) If any document, parcel or thing in the custody of a postal or telegraph authority is, in the opinion of the District Magistrate, Chief Judicial Magistrate, Court of Session or High Court wanted for the

[16] For a general discussion of concerns associated with non-adversarial process to compel data production, *see*, James Orenstein, 'I'm a Judge. Here's How Surveillance is Challenging Our Legal System' (*The New York Times*, 16 June 2019) <https://www.nytimes.com/2019/06/13/opinion/privacy-law-enforcment-congress.html> accessed 19 October 2019.

> purpose of any investigation, inquiry, trial or other proceeding under this Code, such Magistrate or Court may require the postal or telegraph authority, as the case may be, to deliver the document, parcel or thing to such person as the Magistrate or Court directs.
>
> (2) If any such document, parcel or thing is, in the opinion of any other Magistrate, whether Executive or Judicial, or of any Commissioner of Police or District Superintendent of Police, wanted for any such purpose, he may require the postal or telegraph authority, as the case may be, to cause search to be made for and to detain such document, parcel or thing pending the order of a District Magistrate, Chief Judicial Magistrate or Court under sub-section (1).

On a bare reading, Section 91 enables either a court or police officer (of appropriate rank) to issue a summons or written order seeking production of any 'document' or 'thing' that is necessary or desirable for any investigative purpose. Expressly excluded from the scope of this provision are letters, postcards, telegrams, and 'other things' which are in custody of the postal or telegraph authority. Such items may only be seized by order of a judge under Section 92(1) of the Cr.PC. While Section 92(1) manifests a higher level of procedural safeguards in the form of judicial approval prior to issuance of summons, the powers under Section 91, in contrast, may be exercised by a police officer without the need for prior judicial approval.

Another distinction between the two provisions is scope. While Section 91 may be used to compel the production of seemingly anything qualifying as a 'document' or 'thing', Section 92 is more limited in scope – applying only to things in the custody of a postal or telegraph authority.

III. Setting Context: Section 91 and LEA access to Data in Practice

Despite the lack of any specific references to data or electronic evidence, Section 91 is commonly understood to be used by LEA to seek the production of data and other forms of electronic evidence in the possession of intermediaries and other persons.[17] Several authors have noted and com-

[17] Maria Xynou, 'Why 'Facebook' is More Dangerous than the Government Spying on You' (*The Centre for Internet and Society*, 19 November 2013) <https://cis-india.org/internet-governance/blog/why-facebook-is-more-dangerous-than-the-government-spying-on-you> accessed 19 October 2019; Vipul Kharbanda, 'Policy Paper on Surveillance in India' (*The Centre for Internet and Society*, 3 August 2015) <https://cis-india.org/internet-governance/blog/policy-paper-on-surveillance-in-india> accessed 19 October 2019; Elonnai Hickok and Vipul Kharbanda, 'An Analysis of the CLOUD Act and Implications for India' (*The Centre for Internet and Society*, 22 August 2018) <https://cis-india.org/

mented on this practice. For instance, Acharya has noted that the powers under Section 91 may be applied to obtain data at rest such as emails stored in an inbox or sent-mail folder.[18] Similarly, the Centre for Communication Governance has noted that Section 91 is used by LEA to access 'stored data', i.e. data at rest.[19]

While a comprehensive survey of all academic references to Section 91 is outside the scope of this paper, it may be generally acknowledged that several authors express concerns regarding the unilateral ability of LEA to access data under this provision.

In a comprehensive study, Iyengar examines this provision in the context of compelled disclosure of IP addresses. He also studies the relationship between Sections 91 and 92 and notes that it may be possible for Internet Service Providers to be considered as 'telegraph authorities' for the purposes of these provisions – entitling them to the higher standard of protection under Section 92. He also notes separately that "…*Despite their primary functions as email providers, it seems unlikely that any magistrate would interpret webmail providers like Hotmail and Google as "postal authorities" so as to be immune from police summonses under Section 91*…"[20] Overall, he concludes that – given the interpretational uncertainties involved – it would be appropriate to amend the Cr.PC to keep pace with technological developments.[21]

The Centre for Internet and Society too makes similar observations in relation to use of Section 91 to compel production of data.[22] As regards

---

internet-governance/files/analysis-of-cloud-act-and-implications-for-india> accessed 19 October 2019.

18 Bhairav Acharya, 'An Analysis of the Cases Filed under Section 46 of the Information Technology Act, 2000 for Adjudication in the State of Maharashtra' (*The Centre for Internet and Society*, 30 September 2013) <https://cis-india.org/internet-governance/blog/analysis-of-cases-filed-under-sec-48-it-act-for-adjudication-maharashtra> accessed 19 October 2019; *See also*, Amrita Vasudevan and others, 'Law Enforcement Agencies Perceptions of Gender-Based Cyber Violence – An Ethnographic Exploration of Bengaluru City Cyber Police' (*IT for Change*, January 2018) <https://itforchange.net/e-vaw/wp-content/uploads/2018/01/Amrita-Anit-and-Nandini-.pdf> accessed 19 October 2019.

19 Centre for Communication Governance at National Law University, Delhi, 'Comments to TRAI's Consultation Paper on Cloud Computing' (2018) 17 <https://ccgdelhi.org/wp-content/uploads/2018/10/CCG-NLU-Comments-on-TRAIs-Consultation-Paper-on-Cloud-Computing.pdf> accessed 19 October 2019.

20 Prashant Iyengar, 'IP Addresses and Expeditious Disclosure of Identity in India' (2013) 9 Indian Journal of Law and Technology 1, 22.

21 ibid.

22 The Centre for Internet and Society and Privacy International, 'The Right to Privacy in India– Stakeholder Report' (27th Session — India, Universal Periodic Review, 2016) para 17 <https://privacyinternational.org/sites/default/files/2018-04/India_UPR_Stakeholder%20Report_Right%20to%20Privacy.pdf> accessed 19 October 2019.

Section 92 of the Cr.PC, a 2016 report by the organisation also briefly notes that "*…there is little judicial clarity on the subject but it may be argued that it is possible to interpret the provisions in a way that even private ISPs can be considered as postal or telegraph authorities and thus become subject to interception under this section.*"[23]

Separately, Abraham and Hickok make several notable observations about these provisions. For instance, they find that the powers under Sections 91 and 92 are exercised in preference to powers under sectoral frameworks that may also be available to certain LEA.[24] They also note that the breadth of Section 91 has meant that it has been used to request various types of communication data including the content (payload) of communications. In other words, LEA tend to ignore the heightened standards of Section 92 (which the authors suggest is more appropriate) and prefer to use generic Section 91 powers which do not require any form of prior judicial authorisation. Based on inputs from unnamed intermediaries, the authors also report that only basic subscriber information or meta-data is typically provided by intermediaries in response to Section 91 requests since 'communication data' requires a court order under Section 92. However, the authors acknowledge that it is unclear if all intermediaries follow such an approach.[25]

Within this context, in a submission made to the Madras High Court, a leading messaging platform stated that it provides basic subscriber information including "*phone number, name, device info, App version, Start date/time, connection status, last connection date/time/IP, E-mail address, Web client data*"[26] in response to Section 91 requests.

Swire, Hemmings and Srinivasan, among others, have briefly considered Section 91 in the context of cross-border data requests and the requirements of the Clarifying Lawful Use of Overseas Data Act ('**CLOUD Act**') – discussed below. In most such studies, there is general acknowledgement that Section 91 is a key provision under which LEA access to data is effected in India. Relevant to the present analysis, the authors note that "*law enforcement regularly makes use of this broad authority, even continuing to order the production of data under the Cr.PC despite stricter provisions in other specialised statutes like the IT Act and Telegraph Act.*"[27] According to them,

---

[23] ibid.

[24] Abraham and Hickok (n 12) 304.

[25] Abraham and Hickok (n 12) 304.

[26] *Antony Clement Rubin v Union of India* 2019 SCC OnLine Mad 11785 and *Janani Krishnamurthy v Union of India* 2019 SCC OnLine Mad 11785.

[27] Justin Hemmings, Sreenidhi Srinivasan and Peter Swire, 'How Stricter Procedures in Existing Law May Provide a Useful Path for Cloud Act Executive Agreements'

case law suggests "*that this authority has typically been used by the accused, complainants, and prosecutors who would petition the court to compel the production of documents at various stages of a trial.*"[28] Based on their analysis, the authors conclude that a court-issued order under Section 91 would arguably satisfy the CLOUD Act's requirement that an order be independently authorised. As discussed in more detail below, this is only one of the avenues for exercise of powers under Section 91.

Studies also point to several attempted uses of Section 91 which do not seem to flow from the text of the provision. Shora et al. note that Section 91 is often cited in takedown notices which seek *removal of content* alleged to be illegal.[29] Similar efforts to use the provision to censor online content have been noted by SFLC.in.[30]

Overall, it may be noted that several commentators have generally discussed the role played by Section 91 of the Cr.PC in relation to LEA access to data. Some have also touched upon extended uses of Section 91 and the relationship between Section 91 and 92 of the Cr.PC, while fewer have gone as far as to allude to the fact that Section 92 of the Cr.PC may be a more appropriate provision under which access to certain forms of data – such as the contents of communications – may be sought. From the above survey, it may be understood that Section 91 is widely used not only for production orders but also to order other positive acts such as takedown of content. Significantly, several authors cited above have also expressed serious doubts as to the adequacy of the safeguards contained in Section 91.

Despite the above, there has, till date, not been a detailed legal survey surrounding this provision. Much of the above writing (with exceptions) has been from a policy perspective and, therefore, is understandably issue-specific or high-level in nature. The following sections attempt to supplement this existing literature by examining the scope of Section 91 as interpreted by Indian courts. It is hoped that this analysis will be useful to those seeking to understand whether calls for broader reform of the provision are justified.

(*Cross-Border Data Forum*, 16 November 2018) <https://www.crossborderdataforum.org/how-stricter-procedures-in-existing-law-may-provide-a-useful-path-for-cloud-act-executive-agreements/> accessed 19 October 2019.

28 ibid.

29 Shehla Shora and Anja Kovacs, 'Criminalising Dissent? An Analysis of the Application of Criminal Law to Speech on the Internet through Case Studies' (*Internet Democracy Project*, 2013) <https://internetdemocracy.in/reports/criminalising-dissent/> accessed 19 October 2019.

30 'S. 91 of CrPC – the Omnipotent Provision?' (*Software Freedom Law Centre*, 19 March 2013) <https://sflc.in/s91-crpc-omnipotent-provision> accessed 19 October 2019.

IV. Section 91: Key Trends in Jurisprudence

Section 91 has been the subject of extensive judicial analysis. However, as noted by Hemmings and Sreenivasan, much of this has been in the context of applications made to a Court (under this provision) by an accused individual, complainant, or prosecutor seeking orders for certain documents or things to be produced.[31] As this piece is intended to focus on the unilateral powers of LEA to compel production under Section 91 (the likely field for future debate surrounding the provision), it would – at first glance – seem that these decisions are less germane to the present study.

However, this is not necessarily true. For one, several of these decisions enunciate broad principles regarding the exercise of powers under Section 91 generally. As such, they provide valuable guidance on the factors and principles that must also guide the exercise of compelled production powers by LEA under this provision. Further, decisions which discuss the powers of *courts* (to compel production) under Section 91 are also relevant as there is nothing to suggest that the legal standards or burdens in these cases are, in any way, distinct from those applicable to *police* exercising powers under this provision. Where the same power is exercisable in the same circumstances by two different authorities, it is likely that the similar overarching legal principles must govern. Even if this is not found to be the case, the principles applicable to court-ordered production, read in the most favourable light, will likely be required to be satisfied, as a minimum, by police in exercise of powers under this provision.

Lastly, it may also be noted that the focus of this section is on pronouncements which enunciate principles of law which are directly relevant to the application of Section 91 to data or technology. It is not intended to be a comprehensive survey of *all* decisions under Section 91 (or its predecessor provisions). For instance, issues such as the use of Section 91 against accused persons may also raise important questions relating to the right against self-incrimination guaranteed under the Indian Constitution. While potentially relevant in a context where Section 91 powers are sought to be asserted in relation to data in the possession of an accused,[32] broader issues such as these have not been covered here.

---

[31] Hemmings and others (n 27).

[32] These questions may also become relevant in relation to circumstances such as where accused persons are required to unlock or decrypt devices in which relevant data may be stored. However, in such circumstances, LEA may also be able to resort to the more stringent powers available under s 69 of the IT Act (subject to the limitations discussed above in n 15).

A. General Principles

i. Section 91 powers are very wide

It has come to be well-established that the powers and discretion available under Section 91 are extremely wide and only subject to the restriction found in the text of the provision. In *Om Parkash Sharma* v. *CBI*,[33] the Supreme Court noted that the language of the provision would:

> no doubt, indicate the *width of the powers to be unlimited* but the in-built limitation inherent therein takes its colour and shape from the stage or point of time of its exercise, commensurately with the nature of proceedings as also the compulsions of necessity and desirability, to fulfil the task or achieve the object.[34] (emphasis supplied)

In general, in relation to Section 91, a court:

> must be allowed a large latitude in the matter of exercise of discretion and unless in a given case the *Court was found to have conducted itself in so demonstrably an unreasonable manner unbecoming of a judicial authority*, the Court superior to that Court cannot intervene very lightly or in a routine fashion to interpose or impose itself even at that stage.[35]

This decision also demonstrates the legal standard that must be satisfied for an appellate court to properly interfere in a Section 91 order. These observations have been positively cited by a three-judge bench of the Supreme Court in *State of Orissa* v. *Debendra Nath Padhi*.[36] Here, the Supreme Court held that it would be proper to exercise powers under Section 91 only where it has been shown that the persons to whom the summons is addressed hold the records in question and that the same are necessary for purposes of the matter at hand. In other words, the powers under this provision cannot be used for what the Court terms a 'roving enquiry' (discussed below). Regardless, it may be generally inferred that courts and police officers have wide discretion and powers to order production under Section 91. This may particularly have relevance where an LEA order under Section 91 is questioned on grounds of being based on insufficient legal or factual grounds.

While not directly addressed, such discretion is likely to also be available to police officers exercising powers under this provision – which is intended

---

[33] *Om Parkash Sharma v CBI* (2000) 5 SCC 679 (*Sharma*).
[34] *Sharma* (n 33) 684.
[35] *Sharma* (n 33) 684.
[36] (2005) 1 SCC 568: 2004 AIR SCW 6183.

to obviate the need for police to obtain court orders on every occasion where production of any document or thing is required.[37] At the same time, while there is no requirement for judicial pre-authorisation where a police officer issues an order under Section 91, it may be erroneous to suggest that no remedies exist for a target once such an order has been issued. Apart from revision, High Courts may – under their inherent powers – interfere with Section 91 orders where good reasons exist.[38]

ii. Precondition to exercise of powers under Section 91

While the scope of Section 91 is broad, the powers under it are not absolute.[39] A precondition is the formation of a *prima facie* opinion that the document or thing sought to be produced is *necessary or desirable* for the purposes of an investigation or other proceeding under the Cr.PC. In this regard, courts have found that the document or thing called for:

> …must have some relation to or connection with the subject matter of the investigation, inquiry or trial and throw some light on the proceeding or some link in the chain of evidence…In plain words, the documents called for must have some sort of relevancy with the matter under investigation, inquiry or trial.[40]

Therefore, the key requirement to be satisfied is the relatively low standard of 'relevance'. In addition, where Section 91 powers are sought to be exercised by a lower court (Magistrate), this must be on the basis of a *judicial application of mind* to the facts of the case at hand.[41] Similarly, *prima facie* satisfaction must be arrived at by an empowered police officer prior to the issuance of an order under this provision.[42]

Practically, this means that a police officer must have had reasonable preliminary grounds to believe that the document or thing would be useful or relevant for the purposes of a proceeding under the Cr.PC. In other words – based on factors such as the nature and stage of proceedings[43] – it must have been reasonably possible for the officer to preliminarily conclude that

---

37 *CBI v V Vijay Sai Reddy* (2013) 7 SCC 452.

38 *Arun Kumar Kaushik v State of UP* 2013 SCC OnLine All 13023: (2013) 127 AIC 340.

39 Ratanlal and Dhirajlal, *The Code of Criminal Procedure* (21st edn, Lexis Nexis 2018) ch VII; *See also*, *Durga Das v R* 1942 SCC OnLine Lah 69: AIR 1943 Lah 28 *(Das)*.

40 *Subhasini Jena v Commandant of 6th Batallion, OSAP* 1988 SCC OnLine Ori 272: 1988 Cri LJ 1570.

41 Justice ML Singhal (ed), *Sohoni's Code of Criminal Procedure* (22nd edn, Lexis Nexis 2017) 497.

42 *Hussenbhoy Abdoolabhoy Lalji v Rashid B Vershi* 1941 SCC OnLine Bom 10: (1941) 43 Bom LR 523.

43 SC Sarkar, *The Code of Criminal Procedure* (11th edn, Lexis Nexis 2015) ch VII.

production of the concerned document or thing may have a bearing upon the proceeding at hand.[44]

The fact that the produced document or thing does not ultimately turn out to be relevant is of no significance.[45] *At the time of the issuance of the* order under Section 91, a court or empowered police officer must have been able to reasonably conclude that production may be necessary or desirable for investigative purposes.[46] As highlighted in the next section, this low standard may implicate the fundamental right to privacy, as recognised by the Supreme Court in the *Puttaswamy* decision.[47] Correspondingly, without reform, exercise of powers by LEA under this provision may be subject to increasing levels of judicial scrutiny and be set aside on privacy grounds – potentially imperilling evidence collection and investigative functions.

iii. Section 91 requires a written order to be issued by a police officer.

A procedural safeguard that has been built into Section 91 is the need for a written order where a police officer exercises powers under this provision. Within this context, courts have found that a verbal order or instruction issued to any person to produce a document or thing would not suffice.[48] In *Durga Das* v. *Emperor*, the Lahore High Court, in setting aside an order issued under Section 94 of the Code of Criminal Procedure, 1898 ('**1898 Code**')(analogous to Section 91 of the 1973 Code), observed (speaking through Din Mohammad J.):

> …Further I cannot subscribe to the proposition advanced on behalf of the Crown that under Section 94 discretion is vested in a police officer' to issue a written order or not and that if he so chooses, he can demand the production of books in any manner that he likes. If this were so, the provisions of law as contained in Section 94 would be rendered nugatory. The word used is no doubt 'may' but this word has not been used in the sense in which counsel for the Crown takes it to be. It merely means that if a police officer makes up his mind to issue an order to the person concerned, he must do it in writing. Any other interpretation would defeat the object of the Legislature in enacting this provision...[49]

---

[44] *Nizam of Hyderabad v AM Jacob* (1892) ILR 19 Cal 52, 64 (*Jacob*).
[45] *Jacob* (n 44) 64.
[46] Durga Das Basu, *Criminal Procedure Code, 1973* (5th edn, Lexis Nexis 2014).
[47] *KS Puttaswamy v Union of India* (2017) 10 SCC 1.
[48] Basu (n 46); *See also*, *Das* (n 39).
[49] *Das* (n 39) para 6.

Further, it is well-accepted as a general principle of law that, where a statutory provision prescribes a particular procedure in which a power is to be exercised, no deviation from the same is possible. For instance, the Supreme Court in *State of U.P.* v. *Singhara Singh*,[50] explained this rule in the following terms:

> The rule adopted in *Taylor* v. *Taylor*[51] is well recognised and is founded on sound principle. Its result is that if a statute has conferred a power to do an act and has laid down the method in which that power has to be exercised, it necessarily prohibits the doing of the act in any other manner than that which has been prescribed. The principle behind the rule is that if this were not so, the statutory provision might as well not have been enacted.[52] (internal citations omitted)

Therefore, an order issued under Section 91 which is not in writing is likely to be liable to be set aside solely on this ground. In the context of digital evidence sought to be produced, where concerns regarding grounds of proportionality arise, the written order ensures, at the very least, that there is a decision which may be challenged before higher courts.

iv. Non-compliance with order under Section 91

There is no doubt that an order issued under Section 91 is mandatory. The failure to produce a document in pursuance of a Section 91 order would at least amount to the offence of "*failure to produce a document before a public servant by a person legally bound to produce*". Under Section 175 of the Indian Penal Code, 1860, this is punishable with simple imprisonment (for one month), or fine of INR 500, or both.

These negligible penalties for conduct which may have the potential to obstruct or derail an entire criminal investigation only serves to buttress the case for review and reform of Section 91.

---

[50] *State of UP v Singhara Singh* 1964 AIR SC 358 *(Singhara Singh)*.
[51] (1875) LR 1 Ch D 426.
[52] *Singhara Singh* (n 50) para 8.

B. Principles Specifically Relevant to the Production of Data

i. Section 91 orders may be issued to individuals/entities or those holding items on their behalf

An interesting manner in which powers under Section 91 have been interpreted is that orders under the provision need not only be directed to individuals ('**target individuals**') who have in their personal possession, documents or things. Courts have interpreted the powers under this provision to extend to the production of documents and things which are in the control of an individual who is holding the same on behalf of the target individual. As per the author Sohoni:

> The instrument need not be in the actual possession of the party; it is enough if it is his power, which it would be if it were in the hands of a person in whom it would be wrongful not to give up possession to him. But he must have such right to it, as would entitle him not merely to inspect, but to retain it.[53]

For instance, even if an online service provider or intermediary was holding data or information on behalf of an individual, the same would be required to be produced. Such an approach may have crucial implications in the digital era where vast troves of information are stored by third party intermediaries on behalf of individuals.

At the same time, the Supreme Court has found that – where a non-party (to a proceeding) is called upon to produce any document or thing – such a summons or order would not amount to an 'interlocutory' order as a non-party would not have an opportunity to challenge such an order upon completion of proceedings (for example through appeal). Therefore, it was found that such non-parties could maintain revision petitions against such orders[54] – a remedy that is not ordinarily available against interlocutory orders. This line of reasoning has implications for proceedings where intermediaries are themselves not accused or subject of investigation in any matter. In such cases, intermediary entities would retain standing to challenge Section 91 orders where sufficient grounds exist.

---

[53] Singhal (ed) (n 41) 499.

[54] *Parmeshwari Devi v State* (1977) 1 SCC 169: AIR 1977 SC 403.

ii. Inconvenience not a ground for non-compliance with Section 91 order

Where a court or police officer issues an order under Section 91, inconvenience that may be occasioned by compliance with such an order is not a valid excuse for non-compliance. In *Surendra Mohan* v. *K.P.M. Tripathi*,[55] the Allahabad High Court refused to interfere with a Section 91 order issued by a police officer, holding:

> Merely because an order made by the Investigating Officer to produce books of accounts and other things would cause inconvenience to the person from whom it is summoned, it could not be said that the order is beyond the purview of Section 91. Under Section 91 of the Cr.P.C. it is for the Investigating Officer to decide as to whether a particular document or any other thing is necessary or desirable for the purposes of investigation or not. Since there is no material before us to show that the summons was issued by Respondent No. 1 with mala fide intentions, we cannot hold it to be beyond Section 91.

In light of this principle, it may be difficult for individuals or intermediaries who are recipients of a Section 91 order to argue that compliance is overly burdensome or onerous. Where the threshold for production has been met, recipients are bound to produce the documents or things sought. However, it remains an open question of how a court would consider arguments relating to impossibility (rather than inconvenience) to produce data, for example in relation to requests for contents of end-to-end encrypted communications.[56]

iii. Section 91 cannot be used to compel acts other than production

While the text of Section 91 is clear in that it is a means to compel production of *documents* or *things* that may be relevant to an investigation, reports by various organisations (supra) suggest that LEA have attempted to use Section 91 to issue orders requiring positive or negative actions such as the takedown of online content.

---

[55] *Surendra Mohan v KPM Tripathi* 1985 SCC OnLine All 1040: 1986 Cri LJ 1324.

[56] This issue is the subject-matter of ongoing litigation involving various social media platforms before the Madras High Court - WP Nos. 20774 and 20214 of 2018 SCC OnLine Mad 11785 (Madras High Court); *See*, Sameer Sachdeva, 'Impossible to Track Sender of Message due to Encryption: WhatsApp Tells Madras High Court' (*Firstpost*, 11 June 2019) <https://www.firstpost.com/tech/news-analysis/impossible-to-track-sender-of-message-due-to-encryption-whatsapp-tells-madras-high-court-6793561.html> accessed 19 October 2019.

Courts, interpreting previous versions of Section 91 have clearly concluded that this provision would not authorise such actions.[57] In *Prafulla Kumar Deb* v. *Suresh Chandra De*,[58] the Gauhati High Court set aside an order of the Magistrate restraining certain payments through an order under Section 91. The High Court, in relation to Section 94 of the 1898 Code, observed as follows:

> …All that the section authorises is that a document or thing necessary or desirable for the purposes of any investigation, inquiry, trial or other proceeding under the Cr. P.C. may be ordered to be produced. Stopping of payment of certain bills presumably with a view to passing some order with regard to the amount due, to the accused at the termination of the proceedings is evidently not covered by this section….

Similarly, courts have also found that an order directing a bank to prevent an accused from operating his account was not something that could be authorised under *any* provision of the 1898 Code.[59] By implication, it follows that no such order could have been issued under Section 94 – the equivalent to Section 91 of the 1973 Code.

In *Jagdish Prasad Sharma* v. *State of Bihar*,[60] the Patna High Court considered the question of whether an order under Section 91 could compel conversion of the form of things or compel production of a document or thing in a form different to which it ordinarily exists in. In this case, a Magistrate issued an order under Section 91 requiring two bank managers to convert deposited monies into A/C payee drafts in the names of certain individuals. The High Court, setting aside this order, observed:

> …Evidently this section does not authorise the court to direct any person to convert the cash into a Bank draft and that also in the name of a person different from that in whose name the accounts stand. The words used in the section are 'document or thing' which are said to be in possession of the person who is being directed to produce the same. Apparently, this section does not authorise the Magistrate to direct that person to convert the 'thing' in a form different from that in which it was in his possession, Evidently, Section 91 was intended to give an aid in the investigation and trial of the offence under consideration and not for facilitating the disposal of the property involved…So, by this order, the learned Magistrate has not given direction for mere

---

[57] Basu (n 46).
[58] *Prafulla Kumar Deb v Suresh Chandra De* 1950 SCC OnLine Gau 52: AIR 1952 Assam 24.
[59] *Makhan Lal Chatterjee v Emperor* 1935 SCC OnLine Cal 258: (1935) 164 Ind Cas 377.
[60] *Jagdish Prasad Sharma v State of Bihar* 1987 SCC OnLine Pat 258: 1988 Cri LJ 287 (*Sharma*).

> production of the thing or document, but has asked the Managers to produce the same in a different form altogether, which, I am afraid, he was not authorised to do in terms of Section 91 of the Code.
>
> 6. Thus, it is apparent that the learned Magistrate has exceeded his jurisdiction in passing the impugned order, as Section 91 did not authorise him to pass such an order. He could, if necessary, in the interest of trial, direct the Managers concerned to produce the document or thing which he considered necessary to be produced in court, but he could not direct them to change the form of the thing sought to be produced.

This makes clear that Section 91 cannot be used by a court or police officer to compel acts other than the mere production of documents or things. Within this context, guidance offered by key documents such as the (now dated) Data Security Council of India/Deloitte Cyber Crime Investigation Manual – that Section 91 may be used to issue preservation notices/orders– would appear to be *prima facie* incorrect.[61]

Further, an order mandating production cannot require the recipient to fundamentally alter the nature or character of the concerned document or thing prior to production. The powers of magistrates and police officers are circumscribed by the provisions of the Cr.PC and they must act within its four corners.[62] It would be difficult for LEA to justify the use of Section 91, in its current form, to order actions other than production – including takedowns and other positive acts such as blocking or, in an extreme case, key-word based filtering of communications.[63]

iv. 'Documents' and 'Things' refer to *physical* objects

While the 1973 Code itself does not define the term 'document' for the purposes of Section 91, its meaning may be drawn from other contemporary statutes which provide indications as to its general understanding. For instance, the Indian Penal Code, 1860 in Section 29, defines a 'document' in the following terms:

> The word 'document' denotes any matter expressed or described upon any substance by means of letters, figures or marks, or by more than

---

[61] Data Security Council of India and Deloitte, 'India's First Cyber Crime Investigation Manual' (2011) 32, 46 <https://jhpolice.gov.in/sites/default/files/documents-reports/jhpolice_cyber_crime_investigation_manual.pdf> accessed 19 October 2019.

[62] *Sharma* (n 60) paras 5 and 6.

[63] Joseph Menn, 'Yahoo Secretly Scanned Customer Emails for U.S. Intelligence – Sources' (*Reuters*, 4 October 2016) <https://www.reuters.com/article/us-yahoo-nsa-exclusive-idUSKCN1241YT> accessed 19 October 2019.

> one of those means, intended to be used, or which may be used, as evidence of that matter.

Section 3 of the Indian Evidence Act, 1872, also defines a document in similar terms:

> 'Documents' means any matter expressed or described upon any substance by means of letters, figures or marks, or by more than one of those means, intended to be used, or which may be used, for the purpose of recording that matter.

This approach to definition is also found in Section 3(18) of the General Clauses Act 1897. Based on these, it may be observed that there has been a fairly consistent approach to defining 'document' within Indian law. Given that the Cr.PC was enacted in 1973, it is unsurprising that the term 'document' was originally intended to be restricted to a physical document. However, more recently, Indian courts have been open to interpreting the term 'documents' broadly to even include the *electronic contents* stored on various physical media (such as CDs or memory cards) in certain contexts.[64] As discussed below, this trend likely upsets the balance of (LEA and private) interests deemed appropriate by the framers of the Cr.PC and provides further justification for a timely review of Section 91.

In contrast, courts have also suggested that the powers under Section 91 would only extend to the production of *physical* 'things'. In relation to Section 94 of the 1898 Code, the Madras High Court in *T. Subbiah* v. *S.K.D. Ramaswamy Nadar*[65] held, in obiter:

> Section 94, Criminal P.C., will apply only to cases where the Court requires the production of any document or other thing necessary or desirable for the purpose of any investigation, inquiry, trial or other proceeding under the Criminal P.C. In this case, the summons was not issued to the petitioner for the production of any document or any other thing. *The word "thing" referred to in Section 94, Criminal P.C. is a physical object or material and does not refer to an abstract thing.* It cannot be said that issuing of summons to a person for the purpose of taking his specimen signature or handwriting is for the production of any document or a thing contemplated under Section 94, Criminal P.C. (emphasis supplied)

---

[64] For example, in relation to s 207 of the CrPC, *see*, general discussion in *P Gopalakrishnan v State of Kerala* 2018 SCC OnLine Ker 3244.

[65] *T Subbiah v SKD Ramaswamy Nadar* 1969 SCC OnLine Mad 45: AIR 1970 Mad 85.

While the above is not dispositive on the application of Section 91 to data and electronic information, these observations provide insight into how compelled production powers have been understood over time. The provision, in its present form, was undoubtedly only intended to apply to physical documents and objects. Therefore, the procedural safeguards under Section 91 have to be understood to be limited to the context of production of such classes of physical documents and things which originally fit within the definitions above.

While it may be possible to interpret the terms 'document' and 'thing' progressively to include electronic material, such an approach may be ill-advised as it would seek to apply procedural safeguards formulated in the context of physical objects to the electronic domain – where production orders may lead to production of far more material and be significantly more invasive. Such an approach to interpretation would also distort the internal balance between LEA and private interests that were considered appropriate by the framers of the Cr.PC. Further, as discussed in the section below, several considerations extraneous to the text of the Cr.PC may also necessitate revaluating this balance.

v. Roving enquiries are not permitted under Section 91

Courts have consistently held that Section 91 powers cannot be used for 'roving' or 'fishing' expeditions. In practice, this means that the particular document or thing to be produced as well as the person in whose possession the same lies must be clearly specified in an order issued under Section 91.[66] In other words, a 'general direction' to produce all papers relating to any subject will not be enforceable. In *Prankhang* v. *King-Emperor*,[67] the following observations were made on this point:

> …We desire again to point out that the law does not empower a police officer to search an accused's house for anything but the specific article which has been or can be made the subject of summons or warrant to produce. A general search for stolen property is not authorised, and the law cannot be got over by using such an expression as 'stolen property relevant to the case.' Such expressions are vague and misleading and the terms of the law are extremely specific…

As followed in subsequent cases, the document or thing called for must be specified.[68] As discussed below, this reading could raise several issues when

---

[66] *Lotan Bhoji Patil v State of Maharashtra* 1974 SCC OnLine Bom 133: 1975 CriLJ 1577.
[67] *Prankhang v King-Emperor* 1912 SCC OnLine Cal 7: (1911-12) 16 CWN 1078.
[68] Sarkar (n 43).

applied in relation to evidence stored electronically. For instance, it is unclear if a general order to produce all data relating to a specific incident or stored in a specific device would be enforceable. Further, where data is concerned, there is a higher likelihood that a non-particularised or vague order would result in the collection of exponentially more information than a similar order applied in the physical domain.

vi. Privacy as a consideration while issuing orders under Section 91

The level of procedural safeguards included suggest that privacy was not a core consideration of the drafters of Section 91. While there is no doubt that individuals carry far more information on devices like smartphones today, it was still possible for significant amounts of information to be held in physical form in the pre-digital era. A useful analogy concerns a personal diary – which, under most circumstances, could be said to contain significant amounts of personal or intimate information. This analogy was used by the United States Supreme Court in the seminal *Riley* v. *California*[69] case:

> A decade ago police officers searching an arrestee might have occasionally stumbled across a highly personal item such as a diary.…But those discoveries were likely to be few and far between. Today, by contrast, it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives— from the mundane to the intimate.…Allowing the police to scrutinize such records on a routine basis is quite different from allowing them to search a personal item or two in the occasional case.[70] (internal citation omitted)

The fact that Section 91 contained no carveouts for any specific types of sensitive documents or things (such as a diary) would suggest that privacy was not a key consideration at the time of drafting this provision. Or alternatively, that LEA interests in investigation and security were intended to, as a matter of policy, prevail over individual interests such as privacy.

Despite this, with developments in technology and data collection, there seems to have been a handful of cases where courts have *read in* privacy requirements in relation to the exercise of Section 91 powers. In *K. Sureshkumar* v. *C. Sandhumani*,[71] the Madras High Court upheld the order of a lower court declining to order Vodafone to produce "*all call lists and*

---

[69] *Riley v California* 2014 SCC OnLine US SC 71: 189 L Ed 2d 430: 134 S Ct 2473: 573 US (2014).

[70] Riley (n 69) 2490.

[71] *K Sureshkumar v C Sandhumani* Crl OP No. 20741 of 2015 and MP No. 1 of 2015, decided on 18 August 2015 (Mad).

SMS messages" emanating from the mobile number of an individual. The Court held:

> 5. It is seen that for invoking Section 91 Cr.P.C., the petitioner should first satisfy the Court that such a record is available with the person and that the said record is necessary or desirable for the purpose of the case. In *State of Orissa v Debendra Nath Padi*[72], 2004 AIR SCW 6183, the Hon'ble Supreme Court has held that provision of Section 91 Cr.P.C., cannot be used for a roving enquiry.
>
> 6. In this case, the petition filed by the petitioner itself, does not disclose how the SMS details and call details of the complainant is necessary for the just decision of the case. That apart, such call details and SMS details will invade into the privacy of an individual, guaranteed by Article 21 of the Constitution of India and that cannot be infringed via Section 91 CrP.C.

In an analogous fact situation, where the call details and SMS records of an individual were sought to be summoned, the same judge held in *P. Karpagam* v. *N. Mahendran*:[73]

> 4. In the considered opinion of this Court, call details of a person cannot be summoned, just like that at the mere asking, as that would invade the privacy of a person. In the facts and circumstances of this case, especially in a prosecution under Section 138 of Negotiable Instruments Act, call details of the complainant will in no way advance the case of the accused. Hence, this petition is devoid of merits and accordingly dismissed.

The Delhi High Court has also arrived at similar conclusions concerning cell phone records. Interestingly, in *Attar Singh* v. *State (NCT of Delhi)*,[74] the Court affirmed the privacy of a police officer whose call and locational details were sought by an accused for exculpatory purposes. The High Court affirmed and refused to interfere with the decision of the lower court which dismissed the application of the accused:

> …on the ground of non-maintainability as the documents sought to be produced were not part of the charge-sheet and the details of personal telephone of IO/Witness of the case would amount to intrusion in the privacy of the investigating officer.

---

[72] (2005) 1 SCC 568: 2004 AIR SCW 683.

[73] *P Karpagam v N Mahendran* Crl OP No. 12961 of 2016 and Crl MP No. 6702 of 2016, decided on 29 June 2016 (Mad).

[74] *Attar Singh v State (NCT of Delhi)* 2016 SCC OnLine Del 3907.

On revision, the concerned Sessions Court partly dismissed the application by:

> …allowing the preservation of the call data record and location chart of Mobile No. 9818851024 of the petitioner. However, the learned Judge declined to preserve the call data record and location chart of Investigating Officer on the ground of fishing inquiry and intrusion in the privacy of I.O.

Despite the petitioner-accused limiting the request to information concerning two days and affirming that the data summoned could be kept in a sealed cover, the application was refused. The High Court in dismissing the petition, found that the lower court had issued a reasoned order and that there was no cause for interference with the same.

Therefore, it would be wrong to state that there have been no occasions where privacy has been considered in relation to the exercise of powers under Section 91. These decisions, while being the exception rather than the norm, are notable for the fact that they were issued prior to the decision of the Supreme Court in *Puttaswamy* which, with finality, affirmed (or arguably, *reaffirmed*) the constitutional status of the right to privacy under Article 21 of the Constitution of India.

V. The Future of Section 91: What May Lie Ahead

The section above likely constitutes one of the first surveys of the legal principles laid down historically by courts in relation to Section 91 (and its antecedent analogues) insofar as it may be relevant to the compelled production of data in the modern context.

While these principles provide the basis for the discussion to follow, namely what the future may hold for Section 91 of the Cr.PC, questions of judicial interpretation and analysis are unlikely to operate in a vacuum. Equally relevant are legal and policy developments taking place on connected issues such as privacy, data protection, and criminal procedure. Some of these most prominent developments are discussed below. Regardless of how these factors ultimately come to manifest, it is clear that pressing questions remain in relation to the need to reform and review the mechanism under Section 91. As it currently stands, the provision is not efficient to properly serve either individual nor LEA interests.

A. Developments Surrounding the Right to Privacy

A key development which will likely affect the exercise of powers under Section 91 going forward and which calls for its reform is the decision of the nine-judge bench of the Supreme Court in the landmark *Puttaswamy* case where the right to privacy was affirmed to be a fundamental right under the Constitution of India.[75] As per the majority judgment:

> A law which encroaches upon privacy will have to withstand the touchstone of permissible restrictions on fundamental rights. In the context of Article 21 an invasion of privacy must be justified on the basis of a law which stipulates a procedure which is fair, just and reasonable. The law must also be valid with reference to the encroachment on life and personal liberty under Article 21. An invasion of life or personal liberty must meet the three-fold requirement of *(i)* legality, which postulates the existence of law; *(ii)* need, defined in terms of a legitimate state aim; and *(iii)* proportionality which ensures a rational nexus between the objects and the means adopted to achieve them;[76]

Within this context, it remains to be seen if the powers under Section 91 – especially where employed unilaterally by police – would satisfy the test of being fair, just, and reasonable. The broad discretion provided to police to issue orders under Section 91, with no guarantee that privacy will be considered as a ground,is likely to be of specific concern.

In *Puttaswamy* decision, the Supreme Court also seemed to reject the third-party doctrine. Here, the Court appeared to approve the ruling in *District Registrar and Collector* v. *Canara Bank*[77] which it read to hold that:

> the right to privacy is construed as a right which attaches to the person….[it] is not lost as a result of confidential documents or information being parted with by the customer to the custody of the bank" and that "…parting with information (to the bank) does not deprive the individual of the privacy interest.[78]

These observations suggest that orders under provisions such as Section 91 – when addressed to intermediaries – must satisfy the same standards as in cases where they are issued directly to the target individual. In other words, as far as personal privacy is concerned, a lower standard will not

---

[75] *Puttaswamy* (n 47).
[76] *Puttaswamy* (n 47) para 325 (Section T) of Majority judgement.
[77] *District Registrar and Collector v Canara Bank* (2005) 1 SCC 496.
[78] *Puttaswamy* (n 47) para 77 (Section H) of Majority judgement.

likely apply in relation to information entrusted by individuals to third parties such as banks, intermediaries or other organisations.

While there have been instances where Indian courts considered privacy as a ground for interference with Section 91 orders, these have been far and few between. In a post-*Puttaswamy* era, it is likely that this approach will change – with parties more regularly raising privacy-based challenges to orders issued under Section 91. The trickle-down effect of this will also mean that lower courts while issuing orders under Section 91 – will be more likely to consider the impact of summons to produce documents or things, on privacy.

However, likely most contentious will be the application of *Puttaswamy* to the exercise of Section 91 powers by a police officer unilaterally through written order, i.e. without court intervention. It remains to be seen whether a written order issued by a police officer – without any form of judicial authorisation would withstand the test of being "*fair, just and reasonable*" in cases where personal privacy is at issue. The risk of an adverse ruling on this point from an appellate court may result in LEA moving from the issuance of orders unilaterally to approaching courts more often to issue summons where the production of particularly sensitive information is sought. While several possible outcomes exist, none will result in clarity over the provision (and its limits) for either individuals or LEA. For clear and efficient process in the long-term, which ensures respect for privacy and provides a workable mechanism for LEA, legislative review and reform of Section 91 is likely to be required.

Such reform must consider whether safeguards deemed acceptable in 1973 would continue to be appropriate today in light of technological and policy developments. More so as the Court in *Puttaswamy,* at several points, expressed concern over the large-scale data collection by private entities in the digital age. It would be interesting to see if arguments drawing upon these concerns, to argue that Section 91 provides too low a standard of safeguards in production orders, would succeed. Lastly, with the Government in the process of enacting the Personal Data Protection Bill, the interplay between Section 91 powers and this framework is likely to raise several novel issues.

B. Reform to Facilitate Evidence Collection Efforts

Several policy considerations from LEA perspectives may also influence the desirability of reforms to Section 91 of the Cr.P.C.

i. Reform to facilitate cross-border data requests

Of these, a key driver is likely to be the difficulties experienced by Indian LEA in relation to ordering production of data stored in foreign jurisdictions. Presently, Indian LEA must follow the procedure set out in Mutual Legal Assistance Treaties ('**MLATs**') between India and the state from which production is sought. In practice, the complex forwarding mechanism involved and the inadequate resourcing of federal agencies have led to an average delay of 10 months (with exceptions) for obtaining evidence under MLATs.[79] Despite international consensus on the urgent need for reforms to this framework,[80] concrete alternatives for the way forward have yet to emerge.

One proposal that has been gaining traction is the Clarifying Lawful Overseas Use of Data Act ('**CLOUD Act**') which came into force in the United States in March 2018. The CLOUD Act provides an alternative to MLATs for countries seeking production of data stored by US-based companies for predefined investigative purposes. Specifically, the CLOUD Act authorises the U.S. Government to enter into bilateral agreements for cross-border production orders with foreign governments whose legal frameworks satisfy certain criteria. In essence, a foreign government which qualifies under CLOUD Act criteria (and with which a bilateral agreement has been entered) will be permitted to directly serve production requests (through designated LEA) on US-based entities – circumventing the MLAT mechanism.

Of the various criteria required to be satisfied by foreign governments, several pertain to the substantive and procedural legal safeguards which will govern data production requests under the law of the foreign jurisdiction. The following criteria are particularly relevant to issues arising under the 1973 Code and in relation to Section 91:

- Under the CLOUD Act, it is required to be agreed by a foreign government that any order issued by such foreign government *inter alia* "*shall be subject to review or oversight by a court, judge, magistrate, or other independent authority prior to, or in proceedings regarding, enforcement of the order;*"[81]

---

[79] The President's Review Group on Intelligence and Communications Technologies, *Final Report: Liberty and Security in a Changing World* (2013) 227 <https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf> accessed 19 October 2019.

[80] David P Fidler, 'Cyberspace, Terrorism and International Law' (2016) 21(3) Journal of Conflict and Security Law 475 <https://academic.oup.com/jcsl/article/21/3/475/2525373> accessed 19 October 2019; Andrew K Woods (Global Network Initiative), 'Data Beyond Borders – Mutual Legal Assistance in the Internet Age' (2015) 1 <https://globalnetworkinitiative.org/sites/default/files/GNI%20MLAT%20Report.pdf> accessed 19 October 2019.

[81] 18 USC, s 2523(*b*)(4) (2018).

- Under the CLOUD Act, for a foreign government to be eligible to enter into an executive agreement with the United States, it must be able to demonstrate that its legal system "*affords robust substantive and procedural protections for privacy and civil liberties in light of the data collection and activities of the foreign government that will be subject to the agreement*;"[82]
- Further, a factor to be considered in evaluating whether a foreign government's legal system meets the requirements of the CLOUD Act is whether the concerned government "*has adequate substantive and procedural laws on cybercrime and electronic evidence, as demonstrated by being a party to the Convention on Cybercrime, done at Budapest November 23, 2001… through domestic laws that are consistent with definitions and the requirements set forth in chapters I and II of that Convention*."[83] India not being a party to the Convention on Cybercrime, must show equivalency of its extant framework to the standards under the Convention. One such standard is that various law enforcement powers including preservation, data production, and interception be subject to safeguards such as "*judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure*."[84]

Despite the immediate relevance of these requirements to the Section 91 debate, it must be noted that there are several other requirements of the CLOUD Act which are not presently satisfied by Indian law.[85] That said, there may be ways to satisfy the CLOUD Act requirements without substantive reforms to Section 91. For example, as Hemmings and Sreenivasan have suggested, it may be possible for the Indian government to mandate that all requests to be made under a CLOUD Act agreement be routed through courts (as opposed to being unilaterally issued by LEA). Therefore, much of this discussion may be presently academic. However, if India is seeking a more expeditious mechanism for enforcing cross-border data requests, review (and potentially reform) of Section 91 would likely be a necessary precondition.

---

[82] 18 USC, s 2523(*b*)(1) (2018).
[83] 18 USC, s 2523(*b*)(1)(B)(*i*) (2018).
[84] Convention on Cybercrime 2004, art 15(2).
[85] For an analysis of some of these requirements, *see,* Hickok and Kharbanda (n 17).

ii. Reform to clarify LEA powers

In addition to the above, from a LEA perspective, there may be several compelling practical reasons to push for reform to the mechanism under Section 91. For instance, as mentioned above, the current mechanism of orders under Section 91 does not empower police or courts to issue data preservation requests given the inability to issue positive commands under Section 91. The lack of such powers may lead to loss of critical evidence from an investigative or prosecutorial viewpoint.

Another issue on which no clarity has emerged is territorial jurisdiction. It is presently unclear if a police officer – acting under Section 91 – may order production where data is stored outside his district, city, or state. This issue assumes relevance particularly in the context of the rise of cloud computing and remote services which typically result in data being stored within certain metropolitan areas in the country.

Lastly, a key limitation of Section 91 is the negligible framework for penalties for non-compliance with an order or summons issued under the provision. Presently, non-compliance by a non-party to a proceeding is likely to be prosecuted under Section 175 of the IPC in addition to potential proceedings under contempt powers where a court-issued order has been violated. Penalties under this provision may be up to simple imprisonment (for one month), or fine of INR 500, or both. Today, when investigations can turn entirely on electronic evidence, courts may need broader discretion to levy stricter penalties for non-compliance with validly issued production orders.

Therefore, the next iteration of Section 91 may require stricter inbuilt penalties in the form of fines and imprisonment. However, such amendments will only be appropriate where broader reform results in more balanced powers under Section 91.

C. Other Interpretational Issues

A key driver of reform is likely to be the increase in the number of interpretational roadblocks surrounding Section 91. As the analysis above shows, several existing trends in interpretation are not necessarily internally consistent. Further, increased demands for compelled production of data will result in new challenges for LEA.

i. Conflicts of existing interpretations

Under the first category of issues: Section 91 does not lend itself to easy application to data stored electronically. Under one branch of cases (with exceptions), it seems likely that the provision – based on its text – applies only to *physical* objects – and not intangibles. On the other hand, caselaw suggests that orders under Section 91 must be specific and particular in scope. Reading these two principles together may produce anomalous results.

Where *certain* data is sought to be produced, it may be open for the target individual to argue that the production of data– as an intangible – is not recognised within the ambit of Section 91 at all. In order to get around this objection, LEA may use Section 91 to compel production of the relevant physical device or hardware (such as hard disk) housing the data in question. Further, as certain courts have accepted, it may be possible to show that 'documents' includes the electronic contents on such hardware. This may, however, result in a significant amount of unrelated data (housed on the same disk) also being produced – running contrary to the prohibition against roving enquiries and the particularity/specificity requirements that have also developed through caselaw.

Further, under existing case law, it is unclear if LEA can order individuals to copy or convert electronic data into another form for the purposes of production – positive acts which, under existing interpretations, may not be compelled under this provision. Lastly, under similar principles discussed above, even where an entire hard disk is sought to be produced, parties may not be able to take the ground that inconvenience or loss to productivity prevents production.

ii. Emerging interpretations

Under the second category: Significant questions are likely to arise regarding the appropriate substantive legal standards for compelled production of data. In addition to the general concerns discussed above, it may be possible for parties to plausibly argue that – in light of scientific and technological developments since the enactment of the 1973 Code – the mechanism and standard under Section 92 are more appropriate to compel production of data *held by intermediary entities* since they are, in many ways, conceptually similar to postal and telegraph authorities in that they facilitate third-party communication.[86]

[86] Iyengar (n 20).

From an interpretational lens, the question is whether private intermediaries can fall within the ambit of being telegraph or postal authorities – as recognised under Sections 91(3) and 92. While a detailed analysis of this question is beyond the scope of this piece, it must be acknowledged that technological developments have been found to play an important role in the interpretational exercise. In such cases, courts have also been willing to make 'creative' interpretations. For instance, in *State of Punjab* v. *Amritsar Beverages Ltd*., the Supreme Court observed as follows in relation to the seizure of a hard disk under the Punjab General Sales Tax Act, 1948:

> …Information Technology at that time far from being developed was unknown. Constitution of India is a living organ. It had been interpreted differently having regard to different societal situations…. Same principle is applicable in respect of some statutes.
>
> *Creative interpretation had been resorted to by the Court so as to achieve a balance between the age old and rigid laws on the one hand and the advanced technology, on the other.* The Judiciary always responds to the need of the changing scenario in regard to development of technologies. It uses its own interpretative principles to achieve a balance when Parliament has not responded to the need to amend the statute having regard to the developments in the field of science.
>
> Internet and other information technologies brought with them the issues which were not foreseen by law as for example, problems in determining statutory liabilities. It also did not foresee the difficulties which may be faced by the officers who may not have any scientific expertise or did not have the sufficient insight to tackle with the new situation. Various new developments leading to various different kinds of crimes unforeseen by our legislature come to immediate focus. Information Technology Act, 2000 although was amended to include various kinds of cyber-crimes and the punishments there for, does not deal with all problems which are faced by the officers enforcing the said Act…

The recognition of such an approach may provide some basis to widely interpret Sections 91(3) and 92 to apply to internet intermediaries.

Further, there is a general acceptance of the principle that courts must take into consideration developments in science and technology while interpreting statutes.[87] A court may interpret "*a statute according to its current*

---

[87] *Kashmir Singh v Union of India* (2008) 7 SCC 259, citing *Satyawati Sharma v Union of India* (2008) 5 SCC 287; *See also*, *State v SJ Choudhary* (1996) 2 SCC 428, citing Francis Bennion, *Statutory Interpretation* (2nd edn, Butterworths 1986) 288 ("*In construing an*

meaning and applying the language to cover developments in science and technology not known at the time of passing of the statute."[88] With reference to specific developments in technology, the Supreme Court has – in previous cases – "*recognised the progress of science and technology by bringing in line, the scope and meaning of the words and expressions used in existing statutes, with current norms and usage*."[89]

For instance, in *Senior Electric Inspector* v. *Laxminarayan Chopra*,[90] 'telegraph line' (as defined by the Indian Telegraph Act, 1885) was interpreted to include a wireless telegraph having regard to changes in technology. Similarly, in *Laxmi Video Theatre* v. *State of Haryana*,[91] 'cinematograph' (as contained in Section 2(c) of the Cinematograph Act, 1952) was held to cover video cassette recorders and players for representation of motion pictures on television screen.[92]

Interestingly, in relation to Section 92, there may be partial support for such an interpretative approach from an unlikely source – the Andhra Pradesh Police Manual which, in discussing Section 92, notes that "*[t]he reference to Posts and Telegraphs authorities in this section may be interpreted to include Bharat Sanchar Nigam Limited (BSNL) and any other basic telephone (including WiLL) service provider or cellular operator whether Private or Government*."[93] In a way, this accepts Iyengar's argument for private entities to be included with the ambit of 'postal and telegraph authorities' under Section 92.

Therefore, a semblance of a path ahead exists for a court seeking to adopt an interpretation which reads 'postal and telegraph' authorities in a manner

---

ongoing Act, the interpreter is to presume that Parliament intended the Act to be applied at any future time in such a way as to give effect to the true original intention. Accordingly, the interpreter is to make allowances for any relevant changes that have occurred, since the Act's passing, in law, social conditions, technology, the meaning of words, and other matters. Just as the US Constitution is regarded as 'a living Constitution', so an ongoing British Act is regarded as 'a living Act'. That today's construction involves the supposition that Parliament was catering long ago for a state of affairs that did not then exist is no argument against that construction. Parliament, in the wording of an enactment, is expected to anticipate temporal developments. The drafter will try to foresee the future, and allow for it in the wording"). This paragraph of Bennion's work was specifically cited in relation to the CrPC in *State of Maharashtra v Praful B Desai* (2003) 4 SCC 601.

88 *Balram Kumawat v Union of India* (2003) 7 SCC 628.

89 *Hanumant v State of MP* AIR 1952 SC 343: 1952 SCR 1091.

90 *Senior Electric Inspector v Laxminarayan Chopra* AIR 1962 SC 159: (1962) 3 SCR 146.

91 *Laxmi Video Theatres v State of Haryana* (1993) 3 SCC 715.

92 *See generally*, *Rama Pandey v Union of India* 2015 SCC OnLine Del 10484.

93 *Andhra Pradesh Police Manual* (2017) vol IIA 844 <http://www.policetrainingap.org/wp-content/uploads/2017/10/Final-Vol-002A.pdf> accessed 19 October 2019.

more appropriate to the modern context. At the very least, courts are likely to be called on to adjudicate upon these questions in the near future.

Moving away from an interpretational lens, it is also interesting to note that, in relation to Section 95 of the 1898 Code (which is analogous to Section 92 of the 1973 Code), the Law Commission in its 37th Report rejected a recommendation that these powers also be granted to senior police officers:

> 244. With reference to section 96, it has been suggested that powers be given to the Superintendent or Commissioner of Police to require delivery of postal articles, and that power be given to the Deputy Superintendent of Police to order detention, of such articles. We are not able to accept this suggestion. The District Magistrate, being the head of the administration, should have this power, but it is not desirable to give the power to police officers.[94]

This decision speaks to the fact that in a pre-internet (and pre-internet intermediary) era, postal and telegraph communications deserved a higher level of procedural safeguards prior to their detention or production. Further, this statement also arguably speaks to the acceptance of the notion that judicial officers – and not police – would be the more appropriate authority for the exercise of powers where there is a greater chance of sensitive or private information being at issue.

VI. Concluding Thoughts

The above sections constitute what is likely one of the first detailed discussions of the jurisprudence around Section 91 of the Cr.PC in so far as it may relate to questions raised by modern technology and the Internet. Based on the discussions of caselaw above, the following principles may be extracted as being particularly relevant in illuminating the way forward:

(*i*) Powers and discretion available under Section 91 have been interpreted very broadly;

(*ii*) Section 91 orders may be issued to individuals or entities holding *documents* or *things* on behalf of the target individual;

(*iii*) Inconvenience that may be occasioned in production is not a valid ground for non-compliance with an order under Section 91;

---

[94] Law Commission of India, *Thirty Seventh Report on the Code of Criminal Procedure* (December 1967) para 244.

(*iv*) Section 91 cannot be used to order positive actions other than the production of *documents* or *things;*

(*v*) *Documents* and *things,* as contemplated under Section 91, are those which are physical in nature. However, courts are stretching the meaning of 'documents' to also include electronic records stored on physical media;

(*vi*) Orders under Section 91 must be specific and particular. The provision does not permit roving or vague enquiries;

(*vii*) Even prior to the decision of the Supreme Court in *Puttaswamy*, courts have considered privacy concerns while considering orders under Section 91.

In addition to providing guidelines for the usage of Section 91, these principles concurrently outline the case for its reform. As discussed above, several of these principles are no longer relevant in the digital age, others have the potential to excessively invade privacy, while several others internally conflict.[95] Legislative reform is the only path to ensuring a balance between individual rights and LEA powers in a manner that upholds both individual and state interests. In its current form, the provision neither protects privacy nor provides clear and certain procedures for LEA to access evidence stored in electronic form.

A half measure may involve removing the ability of LEA to unilaterally issue orders for production. However, more sustainable reform will entail a comprehensive rebalancing of the various interests at stake. While considerations to ensure respect for privacy are required to be enshrined in the procedural safeguards governing Section 91, a more robust and certain framework for LEA access to data may also be desirable.

Specifically, ensuring that new safeguards (such as the need for judicial authorisation) do not make LEA procedures inefficient or unduly cumbersome will determine the extent of their adoption. In addition, reform must look to equip LEA with additional powers required to tackle the modern demands of criminal investigation. This may include specific provisions enabling preservation requests and clearer guidelines governing the various issues that arise in relation to summons, search and seizure of electronic devices and data. These will be required to account for the increased risk that a court – going forward – will find that insufficient privacy safeguards,

[95] For a general discussion of issues raised by applying 'traditional' frameworks to the electronic/digital domain, *see*, Orin Kerr, 'Digital Evidence and the New Criminal Procedure' (2005) 105 Columbia Law Review 279.

overbroad powers, or vague procedures make evidence acquired inadmissible at trial. A judiciary seeking to extend *Puttaswamy* to its logical conclusion may potentially be called upon to review the wholesale rejection of the exclusionary doctrine by Indian courts thus far. To minimise shocks to the system that may arise from the exclusion of evidence, legislative reform of Section 91 which seeks to comprehensively rebalance the rights of individuals as well as LEA is very much required.

While it is possible that courts will arrive at interpretations or readings of Section 91 which satisfy some of the concerns discussed in this paper, legislative intervention is required to signal a strong commitment to clearer law enforcement powers and their balanced application to scenarios where rights such as privacy and other civil liberties are at issue. Based on the above, a Section 91 of the future (or a Section 91A, if you will) may seek to include the following features:

Recommendations to enshrine privacy interests

(*i*) Requirement for judicial pre-authorisation prior to the issue of a production order – especially where electronic devices and data are at issue; and

(*ii*) Requirement that courts consider personal privacy, proportionality, convenience, and public interest prior to ordering production – especially where electronic devices and data are at issue;

(*iii*) Requirement that production orders are in writing/electronic form, signed, and are as narrowly framed as possible, specific, and particular;

(*iv*) Provision of avenues and grounds of challenge for target individuals (whether through appeal or revision) – regardless of whether they are party to the investigation at issue;

(*v*) Exceptions to the production of data which is subject to legal or other privilege.

Recommendations to clarify LEA powers and improve evidence gathering[96]

(*i*) Express powers for LEA to compel production of physical as well as electronic documents and information;

(*ii*) Stricter penalties for non-compliance with production orders;

---

[96] This categorisation is purely for organisational purposes. It is not, in any way, meant to suggest that privacy and LEA interests are distinct, separate, or mutually exclusive.

(*iii*) LEA powers to order data preservation of data at rest and detention of data in transit – pending judicial authorisation to compel their production;

(*iv*) Authorisation for LEA to issue orders for positive acts *which are required solely to give effect to compelled production orders* (such as to copy/image hard disks which contain relevant material);

(*v*) Where onerous, dragnet, or non-specific orders are required, the court must provide special reasons for their issuance. Further, lower courts must provide an opportunity to appeal their rulings to the High Court prior to their implementation. Alternatively, High Courts may be given jurisdiction so that they may be directly approached by LEA in cases where production orders involve a large number of individuals, are particularly urgent, or are complex to implement.

These suggestions, taken together, may provide the starting point for discussions of a new Section 91 which is oriented towards the digital age and adequately rebalances considerations of privacy, civil liberties, and LEA interests.