CARPENTER V. UNITED STATES: STATE SURVEILLANCE AND CITIZEN PRIVACY

Nehaa Chaudhari and Smitha Krishna Prasad[*]

ABSTRACT

The technological possibility of tracking a mobile phone's location with increasing accuracy coupled with the ubiquity of phones make it possible to track the location of a mobile phone user with considerable accuracy. This increases the potential for intrusive surveillance. This comment analyses the constitutional safeguards against the tracking of such data by the State. First*, it reviews the case* Timothy Ivory Carpenter v. United States*, a United States ("US") judgment on the power of the State vis-à-vis the citizen's right to privacy.* Second*, it compares the principles evolved in the US with Indian jurisprudence.* Lastly*, the comment observes that, despite certain problematic principles from US jurisprudence being eschewed by the Indian Supreme Court, there continues to exist concerns regarding the overreach of State power through Indian statutory provisions and other loopholes that haven't yet been scrutinized from the perspective of the right to privacy.*

[*] Nehaa Chaudhari is Public Policy Lead at Ikigai Law, an award winning policy and law firm focused on emerging technologies. She tweets at @nehaachaudhari. Smitha Krishna Prasad is Associate Director at the Centre for Communication Governance at the National Law University, Delhi, a premier Indian think tank on technology law and policy. She tweets at @smithakprasad. The authors thank Varun Jami, final year law student at Jindal Global Law School, Sonipat, for his editorial assistance..

TABLE OF CONTENTS

I. INTRODUCTION

The United States has 396 million mobile phone service accounts, against a population of 326 million.[1] In India, a country of about 1.3 billion people, the number of mobile phone subscribers stands at over 1 billion.[2] More than half of these will be smartphone users by the end of 2018.[3] Billions of people around the world use mobile phones for a "*wide and growing variety of functions,*"[4] and "*compulsively carry cell phones with them all the time*".[5]

Similar to other disruptive technologies, the mobile phone's design, functionality, technical architecture, and inalienability in modern life has us evaluating how it changes, among others, the relationship between the citizen and the state.[6] In the digital age, citizens and states are constantly renegotiating the terms of their social contract - particularly how citizens' civil rights and liberties stack up against states' police powers - with courts being the final arbiter.[7]

---

[1] Roberts . J., *Timothy Ivory Carpenter, Petitioner v. United States*, 22 June 2018, 585 U.S. ___ (2018).
[2] *More than 5.5 billion mobile users by 2022, India to lead*, HINDUSTAN TIMES (2017), https://www.hindustantimes.com/world-news/more-than-5-5-billion-mobile-users-by-2022-india-to-lead/story-KqCGSfgALYQ4RsMHg7praN.html (last visited Jul 23, 2018).
[3] *India set to have 530 million smartphone users in 2018: Study*, THE INDIAN EXPRESS (2017), https://indianexpress.com/article/technology/india-set-to-have-530-million-smartphone-users-in-2018-study-4893159/ (last visited Jul 23, 2018).
[4] *Carpenter*, Roberts. J., *supra* note 1, at 1.
[5] *Ibid* at 13.
[6] For a discussion on changing relationships of power as a result of disruptive technologies, see, generally, Yochai Benkler, *Degrees of Freedom, Dimensions of Power*, DAEDALUS, THE JOURNAL OF THE AMERICAN ACADEMY OF ARTS & SCIENCES, http://benkler.org/Degrees_of_Freedom_Dimensions_of_Power_Final.pdf (last visited Jul 23, 2018).
[7] *See, generally*, *Puttaswamy v. Union of India*, (2017) 10 SCC 1 (hereafter referred to as *Puttaswamy*) for a detailed overview of disruptive technologies challenging citizen-state relations, and the role that the Indian Supreme Court has played as arbiter, over the years.

Timothy Ivory Carpenter v. United States[8] ("*Carpenter*") is the most recent instance of the Supreme Court of the United States ("SCOTUS") measuring the state's exercise of police powers (search and seizure) against a citizen's right to privacy. The court was called to determine[9] if the state, when it accessed the petitioner's historical cell phone records "*that provide a comprehensive chronicle of the user's past movements*," conducted a "*search*" for the purposes of the Fourth Amendment.[10] In a 5-4 split decision, SCOTUS held that government access of mobile phone records in this case was indeed a Fourth Amendment search,[11] bound by its confines, which include the safeguard of certain expectations of a person's privacy.

In the remainder of this article, we discuss Chief Justice Roberts' majority opinion in *Carpenter,* and its underlying rationale. We compare the law according to *Carpenter* with the Indian position, laid out particularly in *Puttaswamy v. Union of India*[12] ("*Puttaswamy*") and *District Registrar & Collector, Hyderabad v. Canara Bank*[13] ("*Canara Bank*"). We conclude that India does not recognise a broad exception to the right to privacy equivalent to the US' '*third-party doctrine*'. However, the absence of adequate safeguards in Indian laws that provide for government access to personal data of individuals could allow for collection of data on a scale similar to *Carpenter*.

II. *CARPENTER*: PRIVACY CLAIMS IN HISTORICAL CELL-SITE RECORDS

Timothy Ivory Carpenter, the petitioner ("Timothy"), was convicted and sentenced for armed robbery by the court of the first instance, a decision which the Court of Appeals for the Sixth Circuit ("Court of Appeals") upheld. SCOTUS agreed to review the decision, and granted Timothy's petition for a writ of certiorari.[14]

A. Historical Cell-site Records

[8] *Carpenter*, Roberts. J., *supra* note 1.
[9] *Ibid* at 1.
[10] U.S. CONST. amend. IV.
[11] *Carpenter,* Roberts. J., *supra* note 1, at 11.
[12] *Puttaswamy*, *supra* note 7.
[13] *Distt. Registrar and Collector, Hyderabad and Ors. v. Canara Bank and Ors.*, AIR 2005 SC 186.
[14] *Carpenter,* Roberts. J., *supra* note 1, at 4.

At Timothy's trial, the police relied on his historical cell-site location information ("CSLI") to demonstrate that he had been at the place of the robbery while it was taking place. CSLI is a "*time-stamped record*" that a phone generates "*each time [it] connects to a cell-site*".[15] A cell-site consists of a set of radio antennae, and is most often located in mobile phone towers, and sometimes in other places such as building roofs.[16] A mobile phone typically generates multiple cell-site records a minute.[17] It scans the area around, even when not in use (unless it is switched off, or its connection to the mobile network has been disabled), as it tries to connect to the closest cell-site and find the best available signal.[18]

The closest cell-site might be closer than you think it is, and coming ever closer. Mobile network companies, in a bid to ensure better connectivity, are setting up more and more towers and cell-sites. A larger number of cell-sites means that each cell-site has to cover a smaller area.[19] This in turn means that CSLI records are able to pinpoint a mobile phone's location more and more accurately. When coupled with the fact that most cell-phone users are at most only a few feet apart from their cell-phones at all times, CSLI records do not just accurately pinpoint a cell-phone's physical location, but also the user's location.

B. Fourth Amendment Claims and the SCOTUS Ruling

In Timothy's case, the police relied on CSLI records to place Timothy's cell-phone, and as a result, Timothy, at the scene of the crime. The state documented his movements over 127 days, and obtained 12,898 location points.[20] Timothy argued that this constituted a "*search*" for the purposes of the Fourth Amendment.[21] He argued that for a search to be constitutional under the Fourth Amendment, the state was required to obtain a warrant backed by probable cause, which it had failed to do in this case;[22] accordingly, this information ought to be suppressed.

---

[15] *Ibid* at 2.
[16] *Ibid* at 2.
[17] *Ibid* at 2.
[18] *Ibid* at 1.
[19] *Ibid* at 2.
[20] *Carpenter*, Roberts. J., *supra* note 1, at 3.
[21] *Ibid.*
[22] *Ibid.*

Neither the court of the first instance,[23] nor the Court of Appeals agreed with Timothy's argument. The latter opined that Timothy had no "*reasonable expectation of privacy*"[24] in his historical CSLI since he had voluntarily shared that information with his mobile phone network providers.

Having admitted Timothy's appeal, SCOTUS was now required to determine whether or not the state's procurement of Timothy's CSLI violated his Fourth Amendment rights. It had to examine whether the state's action amounted to an unreasonable search or seizure, with a related question being what constitutes a reasonable search or seizure. SCOTUS was required to determine whether Timothy had privacy claims in his CSLI, or, like the Court of Appeals had held, he had no reasonable expectation of privacy.

SCOTUS upheld Timothy's privacy claims, and found that in procuring his historical CSLI, the state had conducted an unreasonable "*search*" for the purposes of the Fourth Amendment.[25] Citing *Katz v. United States*[26] ("*Katz*"), SCOTUS opined that the Fourth Amendment protected "*certain expectations of privacy*" which society was prepared to recognize as reasonable, and not just property.[27] As a result, any state action which intruded upon such an expectation of privacy had to be based on a warrant backed by probable cause.[28] Chief Justice Roberts, writing for the majority, was of the view that while the standard that needed to be met for a search to be acceptable under the Fourth Amendment was one of reasonableness; in almost all cases, a search not pursuant to a warrant backed by probable cause, was likely to be unreasonable.[29] In this case, the state obtained Timothy's information pursuant to a court order obtained under the Stored Communications Act, 1986[30] and not a warrant backed by probable cause. The standard required to be met under this legislation to get a court order is lower than the requirements for a warrant under the Fourth Amendment.[31] As such, the state's action - a warrantless and, therefore, unreasonable search - violated Timothy's Fourth Amendment rights.[32] SCOTUS also noted, however, that although the state could only

[23] *Ibid.*
[24] *Ibid* at 4.
[25] *Carpenter,* Roberts. J., *supra* note 1, at 11.
[26] *Katz v. United States* 389 U.S. 347 (1967). Hereafter referred to as *Katz*.
[27] *Carpenter,* Roberts. J., *supra* note 1, at 5.
[28] SCOTUS discusses *Smith v. Maryland*, *infra* note 45 in *Carpenter*, *supra* note 1, at 2.
[29] *Carpenter*, Roberts. J., *supra* note 1, at 18.
[30] 18 U.S.C. Chapter 121.
[31] *Carpenter,* Roberts. J., *supra* note 1 at 18.
[32] *Ibid* at 3.

access CSLI after obtaining a warrant as a general rule, a warrantless search may be permitted in certain special circumstances.[33]

C. Privacy Principles in Carpenter

When SCOTUS found that the state violated Timothy's Fourth Amendment Rights, it recognised that the amendment protected not just a person's property, but also an expectation of privacy that society was willing to recognize as reasonable. Chief Justice Roberts categorized the issue at hand - privacy interests in a person's physical location data that was maintained by a third party[34] - as bringing together two distinct lines of issues and cases in U.S. privacy jurisprudence. The first of these is about "*a person's expectation of privacy in his physical location and movements*"[35] and the second is about the '*third-party doctrine*' and "*whether there is a 'legitimate expectation of privacy' in information [that a person] voluntarily turns over to third parties*".[36]

The judgment in *Carpenter* follows from SCOTUS' landmark 2012 decision on locational privacy in *Jones v. United States*[37] ("*Jones*"). In *Jones*, the issue was whether the state had violated the respondent's privacy by remotely monitoring his vehicle's movements for 28 days, via a GPS tracking device that they had installed on it.[38] In *Carpenter*, Chief Justice Roberts observes[39] that although the decision in *Jones* was based on "*physical trespass of the vehicle*" by the state, five SCOTUS Justices shared the view that the case raised privacy concerns on at least two fronts - by law enforcement "*surreptitiously activating a stolen vehicle detection system*" and by tracking the GPS location of the respondent's mobile phone.

SCOTUS' observations on GPS tracking in *Jones* are particularly important for *Carpenter*. In fact, the majority in *Carpenter* views the threat to privacy from government access of historical CSLI to be far greater than the threat to privacy from GPS surveillance in *Jones*.[40] This is because of three reasons. First, in the words of Chief Justice Roberts, "*[w]hen*

[33] *Ibid* at 4.
[34] *Ibid* at 7.
[35] *Ibid* at 7.
[36] *Ibid* at 9.
[37] *Jones v. United States*, 565 U. S. 400 (2012).
[38] *Carpenter*, Roberts. J., *supra* note 1, at 8.
[39] *Ibid.*
[40] *Ibid* at 13.

the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user".[41] Second, because the information is historical as well as records are continuously logged, by accessing historical cell-site records the state can effectively "*travel back in time*"[42] and recreate in some detail a person's movements and location history. Third, because all mobile phones continuously generate CSLI, the state's ability to track such information *"runs against everyone*" and the only ones who can "*escape this tireless and absolute surveillance*" are the few people who do not have a mobile phone.[43] Chief Justice Roberts also notes that while deciding cases involving state surveillance with implications for the Fourth Amendment, the court's approach needs to be future-proof and technology neutral.[44]

SCOTUS' holding in *Jones* notwithstanding, the question of privacy claims in historical cell-site records is complicated as a result of a second line of cases about the '*third-party doctrine*'. The most important of these are *Smith v. Maryland*[45] ("*Smith*") and *United States v. Miller*[46] ("*Miller*").

Simply put, under the '*third-party doctrine*', a person has a "*reduced expectation of privacy*"[47] in information that she voluntarily discloses to a third party.[48] As a result of *Miller*, the position in U.S. law is that this reduced expectation of privacy will apply regardless of the fact that the person may have disclosed it for a limited purpose.[49] In *Miller*, the state had subpoenaed many of the respondent's bank records including monthly statements, deposit slips and cancelled cheques[50] as it was investigating him for evading his taxes.[51] SCOTUS did not uphold the respondent's Fourth Amendment claim. It held that the documents subpoenaed were not confidential but were "*business records of the banks*"[52] and that when he disclosed this information to the bank, the respondent had assumed the risk that the bank would disclose that

[41] *Ibid* at 13.
[42] *Ibid* at 13.
[43] *Ibid* at 14.
[44] *Ibid* at 6, 14 and 15. SCOTUS refers to *Kyllo v. United States*, 533 U. S. 27, 34 (2001).
[45] *Smith v. Maryland*, 442 U. S. 735 (1979).
[46] *United States v. Miller*, 425 U. S. 435 (1976).
[47] *Carpenter*, Roberts. J., *supra* note 1, at 3.
[48] *Smith*, *supra* note 45; *Miller*, *supra* note 46, and *Ibid* at 3.
[49] SCOTUS cites *Miller* in *Carpenter*, Roberts. J., *supra* note 1, at 9.
[50] *Ibid.*
[51] *Ibid.*
[52] *Ibid.*

information to the state.[53] Similarly, in *Smith*, SCOTUS found that the petitioner having voluntarily communicated to the phone company telephone numbers that he had dialled, had "*assumed the risk*"[54] that the company would share its records with the state.[55]

The majority in *Carpenter* declined[56] to uphold the state's argument that its collection of Timothy's historical cell site information was governed by the '*third-party doctrine*'. It differentiated between CSLI and the "*limited types of personal information*" that was in question in *Smith* and *Miller* - telephone numbers and bank records, respectively.[57] SCOTUS also opined that the third-party doctrine could not "*mechanically*" be applied to CSLI, given "*the lack of comparable limitations on the revealing nature of CSLI*".[58] It also found no element of voluntariness in subscribers sharing mobile phone location information with their telecom service providers:[59] as mentioned earlier in the paper, mobile phones are constantly generating cell-site records as long as they are not switched off/their mobile network connectivity is not disabled; and mobile phones have become an indispensable part of our lives today.[60]

Bringing together the law on locational privacy developed in *Jones* and other cases, and the law on the '*third-party doctrine',* in *Carpenter,* SCOTUS held "*an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI*".[61] However, it did not explicitly overrule the *third-party doctrine*.

III. INDIAN LAW IN THE CONTEXT OF *CARPENTER*'S PRINCIPLES

The Indian Constitution does not have a provision similar to the Fourth Amendment. Article 20(3) of the Indian Constitution only contains a protection against self-incrimination: "*No person accused of any offence shall be compelled to be a witness against himself*". In *M. P. Sharma v. Satish Chandra, District Magistrate, Delhi*[62] ("*M. P. Sharma*") the Supreme Court held that in the absence of a provision similar to that of the Fourth Amendment to the

[53] *Ibid* at 10.
[54] *Ibid.*
[55] *Ibid.*
[56] *Ibid* at 11.
[57] *Ibid.*
[58] Carpenter, Roberts. J., *supra* note 1, at 3.
[59] *Ibid.*
[60] *Ibid* at 11.
[61] *Ibid.*
[62] *M. P. Sharma v. Satish Chandra, District Magistrate, Delhi,* (1954) SCR 1077.

US Constitution, the right to privacy cannot be read into the provisions of Article 20(3) of the Indian Constitution.

This case has, however, been partially overruled by the Indian Supreme Court ("Supreme Court") in *Puttaswamy*.[63] In this landmark judgment, the Supreme Court upheld and confirmed that the right to privacy is a fundamental right under the Indian Constitution. Although the Indian Constitution does not explicitly recognise such a right, the Supreme Court in *Puttaswamy* found that "*[t]he right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution*". In this vein, the Court also overruled *M. P. Sharma* to the extent that it held that the right to privacy is not protected by the Constitution.

The *Puttaswamy* judgment is a milestone in Indian privacy jurisprudence. A 9-judge bench of the Supreme Court upheld the right to privacy as a fundamental right. The primary opinion in this judgment, authored by Justice Chandrachud, and signed by 3 other judges, also recommended that the State ensure that the regulatory framework in the country support the exercise of this right, and specifically the right to data privacy.

However, to understand the position of Indian jurisprudence in the context of the facts and principles discussed in Carpenter, we look at two previous judgments of the Supreme Court: *People's Union for Civil Liberties v. Union of India*[64] ("*PUCL*") and *Canara Bank*, and corresponding legal provisions. The first deals with the interception and monitoring of telephone communications, and the second with search and seizure of records held by third parties. Both of these judgments have been discussed in detail and upheld in *Puttaswamy*.[65]

A. Interception of Communications and the PUCL Judgment

The Indian state's powers to conduct surveillance, and search or seize documents and records are governed by multiple statutory frameworks. The Telegraph Act, 1885 ("Telegraph Act") is among the more comprehensive of these statutes. The provisions of the Telegraph Act

[63] *Puttaswamy, supra* note 7.
[64] *People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301. Hereafter referred to as *PUCL*.
[65] *Puttaswamy*, *supra* note 7.

and rules issued under this law govern the State's powers to intercept telephone communications.

Section 5(2) of the Telegraph Act provides that the government may intercept telephone communications, among other things, in the event of any public emergency, or in the interest of public safety. Such action can only be undertaken if the government is satisfied that interception of such communication is necessary in the "*interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of an offence*". Reasons for directing such interception must be recorded in writing.

In *PUCL*,[66] this section was challenged as unconstitutional before the Supreme Court. The Supreme Court upheld the section, but also provided guidelines on the circumstances and manner in which telephone communications may be intercepted under Section 5(2) of the Telegraph Act. It directed that:[67]

1. Telephone-tapping orders under Section 5(2) of the Telegraph Act can only be issued by the Home Secretary, Government of India (Central Government) and Home Secretaries of the State Governments. This power can be delegated to officers in the Home Department, who are at least of the rank of Joint Secretary in case of emergencies. Copies of each order should be sent to the Review Committee (see below), within a week.
2. The order should direct interception of the communications described in the order, and may also direct the disclosure of such intercepted materials to specific persons.
3. The order should be issued only after considering whether the information to be obtained by such interception cannot be reasonably acquired by other means, and should direct limited interception of communications between specific address(es) and persons / premises.
4. Any order for interception will be valid for 2 months, unless renewed. The total period for which one order can operate is 6 months.
5. The authority issuing the order should maintain records of the intercepted communications, the extent to which the material is disclosed, the number of persons

[66] *PUCL*, *supra* note 64.
[67] *Ibid.*

and their identity to whom any of the material is disclosed, the extent to which the material is copied and the number of copies made of any of the material.

6. The use of the intercepted material should be limited to a necessary minimum, and any copies of intercepted material must be destroyed as soon as retention is no longer necessary.
7. A Review Committee will be set up at both Central and State levels.
    a. The review committee must investigate whether each order passed under Section 5(2) was relevant, and passed in accordance with the terms of Section 5(2) within 2 months of the order.
    b. If the committee finds that an order was passed in violation of Section 5(2), the order will be set aside, and intercepted material must be destroyed.

The Supreme Court did not however impose procedural requirements, i.e. there is no requirement for a search warrant or prior judicial scrutiny to intercept / obtain intercepted material.[68]

The guidelines provided by the Supreme Court were modified slightly, and codified by way of Rule 419-A of the Indian Telegraph Rules, 1951. In addition to the provisions and rules under the Telegraph Act, we also see that the Information Technology Act, 2000 ("IT Act") touches upon interception and monitoring of content.

Section 69 of the IT Act provides the central and state governments with the power to intercept, monitor or decrypt any information[69] generated, transmitted, received or stored in any computer resource.[70] The government may order interception, monitoring or decryption of information where necessary in the interests of the "*sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence*". This list of reasons is largely similar to that under Section 5(2)

[68] Chaitanya Ramachandran, *PUCL v. Union of India revisited: Why India's surveillance law must be redesigned for the digital age*, NUJS Law Review, 7 NUJS L. Rev.105 (2014), http://nujslawreview.org/2016/12/04/pucl-v-union-of-india-revisited-why-indias-surveillance-law-must-be-revised-for-the-digital-age/ (last visited Jul 23, 2018); Chinmayi Arun, *Paper-Thin Safeguards and Mass Surveillance in India*, 26 NLSI REV. 105 (2014), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2615958 (last visited Jul 23, 2018).

[69] Section 2(1)(v) - Definition of Information: "includes [12] [data, message, text], images, sound, voice, codes, computer programmes, software and data bases or micro film or computer generated micro fiche."

[70] Section 2(1)(k) - Computer resource is defined to include a 'computer, computer system, computer network, data, computer data base or software', most of which are defined terms under the IT Act.

of the Telegraph Act, with the notable additions being the defence of India, and investigation of any offence.

The other notable difference between the provisions of the Telegraph Act and the IT Act, is that orders for interception, monitoring or decryption, under the IT Act, can be issued at any time subject to the list of acceptable reasons for such order discussed above. However, the Telegraph Act requires additional circumstances involving public emergency, or public safety to be present before such orders are issued.

Section 69B of the IT Act also empowers the government to authorise the monitoring and collection of traffic data or information generated, transmitted, received or stored in any computer resource. Such monitoring and / or collection maybe undertaken to enhance cyber security and for identification, analysis and prevention of intrusion or spread of computer contaminant in the country. Both, Sections 69 and 69B, as well as the rules[71] issued under these sections, provide procedural guidelines that need to be followed with regard to orders issued under these sections.

B. The Search and Seizure of Records and the Canara Bank Judgment

In *Canara Bank,*[72] the Supreme Court examined the validity of laws that permitted inspection and seizure of documents held by a third party public institution. Stamp laws in India typically require a duty to be paid on the execution of certain documents. The authorities under the local stamp law in the state of Andhra Pradesh were empowered to inspect documents held by public institutions, to examine whether the appropriate duty had been paid. In this case, the question was whether this power could be used to inspect and seize agreements / documents provided by individuals to public sector banks (to which the bank was not necessarily party); for instance, for the purpose of securing a loan.

In its judgment in *Canara Bank*, the Supreme Court discussed the right to privacy *vis-a-vis* search and seizure laws, the debate around the *third-party doctrine* in the US, and similar

[71] Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009 and Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009.
[72] *Canara Bank*, *supra* note 13.

debates in other countries. It upheld the decision of the Andhra Pradesh High Court, which found that the provision in question was unconstitutional on the following grounds:

1. the provision was inconsistent with the other provisions of the State's stamp laws;
2. the provision was violative of the principles of natural justice;
3. the provision was arbitrary and unreasonable and hence violative of Article 14 of the Constitution; and
4. the provision was arbitrary, and unreasonable, and could be considered an excessive delegation of statutory powers, since it did not provide any guidelines for the exercise of power by authorized persons.

Below we look into the primary legislative provisions that govern search and seizure powers, and the Court' discussion on privacy in its judgment in *Canara Bank*.

C. Legal Provisions on Search and Seizure

The primary legislation dealing with search and seizure of documents in India is the Code of Criminal Procedure, 1973 ("CrPC"). The relevant provisions dealing with such powers, as discussed by the Supreme Court in *Canara Bank*, are described below.

Section 93 of the CrPC allows a court to issue a search warrant in specific circumstances, for instance where the court has issued a summons / requisitioned a document and believes that such an order will not be followed, or an inquiry / trial will be served by a general search or inspection. The court may specify the place (or part of the place) that needs to be searched or inspected under such a warrant.

Section 92 of the CrPC also allows District Magistrates and Courts to require a postal / telegraph authority to deliver any document, parcel or things within their custody, that the District Magistrate or Court deems necessary for any investigation, inquiry, trial or other proceeding.

Section 165 of the CrPC allows a police officer authorised to investigate an offence, to search a place within their jurisdictional limits, if the officer believes that "*anything necessary for the purposes of an investigation ... may be found in any place with the limits of the police station of which he is in charge, or to which he is attached, and that such thing cannot in his*

opinion be otherwise obtained without undue delay". The officer may conduct such a search or authorise a subordinate to conduct the search after recording reasons for their belief, and specifying to the extent possible the thing that they are searching for, in writing.

The Court also noted that other laws such as the Income Tax Act, 1961 also contain provisions regarding the search and seizure of documents[73].

D. Privacy Jurisprudence in Canara Bank

Looking into international human rights law, US and other foreign jurisprudence, as well as precedents set by the Indian Supreme Court, the Court in *Canara Bank* traced the evolution of the right to privacy - beginning as a right to property, and eventually being recognised as a right in relation to a person.

For this purpose, the Court referred to SCOTUS judgments in *Warden v. Heyden*,[74] where it was "*recognized that the principal object of the Fourth Amendment is the protection of privacy rather than property*". The Court also referred to *Katz,*[75] which reiterated that the Fourth Amendment protects people and not places.

Tracing the evolution of the right in India, the Supreme Court referred to its early cases, specifically to *Kharak Singh v. State of UP*,[76] noting that the right to privacy was held to be part of the right to life under Article 21 in this case. The Court also referred to *Govind v. State of MP*[77] ("*Govind*") which found that the right to privacy has been implied in Article 19(1)(a) and (d) and Article 21 of the Constitution.

Moving to the facts in question in *Canara Bank*, the Court noted that that in a situation where a bank holds documents of its customers, there is an element of confidentiality in the relationship between the bank and the customer. Here, the Court questioned the right of the State to inspect or seize such documents without any prior reliable information supporting the inspection.

[73] Section 132 and 133 of the Income Tax Act, 1961.
[74] *Warden v. Heyden* (1967) 387 US 294 (304).
[75] *Katz*, *supra* note 26.
[76] *Kharak Singh v. State of UP*, 1964 (1) SCR 332.
[77] *Govind v. State of M.P.*, [1975] 2 SCC 148.

In this context the Court specifically referred to the '*third-party doctrine*', and the principle of '*assumption of risk*' as laid out by SCOTUS in *Miller*. The Court noted however, that the decision in *Miller* was criticised by jurists, on the basis that this third-party doctrine was "*based on the old concept of treating the right of privacy as one attached to property whereas the Court had, in Katz accepted that the privacy right protected 'individuals and not places*".[78]

The Court also noted that the Right to Financial Privacy Act, 1978[79], was enacted post *Miller*. This law "*provided several safeguards to secure privacy, namely requiring reasonable cause and also enabling the customer to challenge the summons or warrant in a Court of law before it could be executed.*"

Reiterating that in *Govind*, and later cases, the Supreme Court has held that the right to privacy deals with persons and not places. The Court stated that "*we cannot accept the line of Miller in which the Court proceeded on the basis that the right to privacy is referable to the right of 'property' theory*". The Court found that the search of documents in the given circumstances could not be valid unless there was some probable or reasonable cause.

This judgment of a 2-judge bench in *Canara Bank* has been discussed in detail, and upheld (among several other judgments), by the 9-judge bench of the Supreme Court in *Puttaswamy.*[80] Discussing *Canara Bank*, the Court in *Puttaswamy* found that the decision in *Canara Bank* has important consequences for recognising informational privacy for the following reasons:[81]

> "*The significance of the judgment in Canara Bank lies first in its reaffirmation of the right to privacy as emanating from the liberties guaranteed by Article 19 and from the protection of life and personal liberty under Article 21 … Thirdly, the right to privacy is construed as a right which attaches to the person. The significance of this is that the right to privacy is not lost as a result of*

[78] *Canara Bank*, *supra* note 13.
[79] *Ibid. See also,* Right to Financial Privacy Act, 12 U.S.C. §§ 3401-342.
[80] *Puttaswamy*, *supra* note 7.
[81] *Puttaswamy*, Chandrachud. J., *supra* note 7, at para 65.

confidential documents or information being parted with by the customer to the custody of the bank ... Fourthly, the Court emphasised the need to read procedural safeguards to ensure that the power of search and seizure of the nature contemplated by Section 73 is not exercised arbitrarily. Fifthly, access to bank records to the Collector does not permit a delegation of those powers by the Collector to a private individual ... Sixthly, information provided by an individual to a third party (in that case a bank) carries with it a reasonable expectation that it will be utilised only for the purpose for which it is provided ... Seventhly, while legitimate aims of the state, such as the protection of the revenue may intervene to permit a disclosure to the state, the state must take care to ensure that the information is not accessed by a private entity".

IV. CONCLUDING OBSERVATIONS

The Indian Supreme Court's judgment in *Canara Bank* clearly states that the right to privacy under Indian law applies in relation to a person, and not in relation to property or a place. This position has been reiterated by the Court in *Puttaswamy.*[82]

The *Canara Bank* judgment is also clear that a US style third-party doctrine doesn't apply in India.[83] However, the right to privacy vis-a-vis the state's power to search, inspect or seize documents and collect information still needs to be examined on a case to case basis. In *Canara Bank*, the court addresses the need for procedural safeguards to the state's powers of search and seizure, both in its discussion of the criticisms of *Miller* and the *third-party doctrine*, as well as in the specific context of the impugned law in the case.

Some of the older provisions permitting search and seizure of documents under the CrPC have been tested in court, and the scope and limitations of these provisions have been discussed in detail.[84] However, the various provisions and rules that do permit interception of communications and collection of information under the Telegraph Act and the IT Act have

[82] *Ibid* at para 168.
[83] *Canara Bank*, *supra* note 12.
[84] *Ibid.*

been criticized for their lack of adequate safeguards.[85] In the absence of proper safeguards, a *Carpenter* like scenario where the state is empowered to collect large amounts of information is entirely possible under existing laws in India.

At the time of writing this paper, we await the recommendations of the Committee of Experts set up to provide recommendations on a legal framework for data protection in India[86] ("Committee"). In November 2017, this Committee published a white paper outlining the various issues that the Committee found important to incorporate into the law, and solicited public comments on these issues.[87] This white paper notes that a comprehensive data protection law should be applicable to the collection and processing of data by both private actors and the State.[88] It then goes on to provide that exceptions should be made under this law, for the purpose of law enforcement and national security.[89] However, there is almost no discussion on the nature of the exception or the safeguards that should be put in place in this context.

Any conversation on the protection of personal information of individuals, should necessarily include the protection of such information against arbitrary collection and processing of data by the State - whether for law enforcement purposes or otherwise. Given the Committee's view that there is need for a comprehensive data protection law that applies horizontally across sectors,[90] it would be useful for this Committee to discuss collection and processing of data by the State in all contexts.

It could be argued that issues such as surveillance, law enforcement and national security are outside the purview of the Committee's mandate. However, we note that the Committee has not shied away from discussing these issues in the context of data localisation and cross border transfer of data - situations where the interests of the State may be affected.[91]

---

[85] *Supra* note 68. See also Sunil Abraham, Elonnai Hickok; Government access to private-sector data in India, *International Data Privacy Law*, 2 (4), 302–315, (November 1, 2012), https://doi.org/10.1093/idpl/ips028 (last visited Jul 23, 2018).
[86] Ministry of Electronics and Information Technology, *Office Memorandum No. 3(6)/2017-CLES*, http://meity.gov.in/writereaddata/files/MeitY_constitution_Expert_Committee_31.07.2017.pdf (last visited Jul 23, 2018).
[87] Ministry of Electronics and Information Technology, *White Paper of the Committee of Experts on a Data Protection Framework for India,* (2017), http://meity.gov.in/white-paper-data-protection-framework-india-public-comments-invited (last visited Jul 23, 2018).
[88] *Ibid* at 31.
[89] *Ibid* at 57.
[90] *Ibid* at 31.
[91] *Ibid* at 69.

With 396 million mobile phone service accounts in the US,[92] SCOTUS has taken cognizance of the impact that phone-based location tracking could have on one's privacy, in an age where tracking a mobile phone could lead to "*near perfect surveillance*."[93] India on the other hand has over a billion mobile phone accounts,[94] several surveillance regimes comparable to those in the US,[95] and limited (if any) safeguards protecting the rights of its citizens. If the fundamental right to privacy, as discussed in *Puttaswamy* is to be upheld in a meaningful manner, it is imperative that adequate safeguards that stand the tests of constitutionality are built into the way in which the State interacts with citizens' personal information.

[92] *Carpenter*, Roberts. J., s*upra* note 1.
[93] *Ibid* at 13.
[94] *Supra* note 2.
[95] Privacy International and Centre for Internet and Society, *State of Privacy in India (January 2018)*, https://privacyinternational.org/state-privacy/1002/state-privacy-india (last visited Jul 23, 2018).