NLUJ Law Review

Rigved Prasad. K, *Procuring Digital Evidence and the Metaphor Problem: Assessment of India in Comparison to USA, Canada and UK*, 8(1) NLUJ L. REV. 131 (2021).

PROCURING DIGITAL EVIDENCE AND THE METAPHOR PROBLEM: ASSESSMENT OF INDIA IN COMPARISON TO USA, CANADA AND UK

*Rigved Prasad. K**

ABSTRACT

Search and Seizure are a part and parcel of investigations, and the State has legitimate interest in detecting and preventing crimes. Such powers during investigations enable the law enforcement to effectively produce evidence for prosecution and obtain convictions. The development of technology, however, has disrupted this seemingly seamless process of investigation. This is mainly because digital evidence is inherently different from traditional documentary evidence. This fundamental difference demands a deviation from traditional conceptions of privacy and the need to conceptualise new developments such as reasonable expectations of one's anonymity and control of customer information vis-à-vis a third party and many other implications on privacy that digital evidence presents. Instances in which the State could obtain data and the

* The author is a junior associate at BFS Legal, Chennai and may be contacted at **rigvedprasad98@gmail.com**. The author would like to thank their colleague and friend Shrayashree Thiyagarajan, Advocate, Madras High Court, for immensely aiding the author for defining the aim and scope of the paper. The author would also like to extend their gratitude towards Ms. Indumugi C, a final year law student at Tamil Nadu National Law University for their invaluable inputs and insightful suggestions.

criminal procedure applicable would determine whether such intrusion would be reasonable intrusion or not. India's jurisprudence on privacy itself is still in the stage of its infancy. Therefore, it is relevant and necessary to ascertain and analyse how other jurisdictions such as USA, Canada and the UK have conceptualised privacy in light of these new developments and managed to balance the competing rights of an individual and the legitimate state interest. This paper aims to ascertain the effectiveness and the shortcomings of the existing procedure in India to procure digital evidence in comparison to the principles and procedure existing in USA, Canada and UK.

TABLE OF CONTENTS

I. INTRODUCTION

Living in the age of data driven capitalism, it is hard to ignore the enormous amount of information of a person contained in personal electronic devices and remote servers of Internet Service Providers [*hereinafter* "**ISPs**"]. Privacy has to be protected from both State and non-State actors.[475] In corollary, these mammoth repositories of personal information and the constitutional implications of its accessibility to State come into play during criminal investigations.

The absence of data protection law in India has left the right to privacy in a limbo. For instance, while the Supreme Court of India [*hereinafter* "**the Supreme Court**"] required the legislature to put in place a sophisticated legal framework to ensure transparency and accountability of the Aadhaar Scheme;[476] the Aadhaar (Targeted Delivery of Financial and other subsidies) Act, 2016 [*hereinafter* "**Aadhaar Act**"] suffers from major conflicts of interest and excessive delegation, and the Rules thereof appear to be in blatant ignorance of the safeguards suggested in the judgement.[477] Similarly, the infamous Encryption Policy, 2015 that was notified by the Government of India (now withdrawn), mandated every citizen and intermediary to retain an unencrypted message for about 90 days, and

---

[475] *See* Vrinda Bhandari & Renuka Sane, *Protecting citizens from the State post-Puttaswamy: Analysing the Privacy Implications of Justice Srikrishna Committee and the Data Protection Bill, ,* 14(2) SOC-LEG REV. 2018 143, 149-150 (2018); *see also,* K. S. Puttaswamy v. Union of India, (2017) 1 SCC 1, ¶ 328. ("***Privacy Judgement***").

[476] *Id,* 510.

[477] *See generally,* Vrinda Bhandari & Renuka Sane, *A Critique of Aadhaar Legal Framework*, 31 NAT'L L SCH INDIA REV. 22 (2019).

further also mandated intermediaries to share their decryption keys in the garb of licensing, essentially rendering encryption and the use of it inconsequential.[478]

Contrary to popular belief, encryption was not specifically invented to facilitate crime but was only a natural result of the internet transforming from a trust-based community to a non-trust-based platform of communication.[479] Therefore, intermediaries have economic interests in facilitating encryption in their services and devices, and hence resist dilution of encryption.[480] This resistance can also be inferred from Apple Inc. refusing to decrypt an iPhone of an accused when FBI requested it to do so.[481] Right to encryption has also been internationally recognised as a fundamental right due to its ability to provide anonymity to a person in cyberspace.[482] Unfortunately, this facility is also being used for crimes, which the law enforcement terms as the "Going Dark" problem.[483] Therefore, there arises a situation where law enforcement has to depend on

---

[478] Bedavyasa Mohanty, *"Going Dark" in India: The Legal and Security Dimensions in India,* ORF OCCASIONAL PAPER, (Dec. 13, 2016), https://www.orfonline.org/research/going-dark-in-india-the-legal-and-security-dimensions-of-encryption, at 4. ("**Bedavyasa Mohanty**")

[479] Justin (Gus) Hurwitz, *Trust and Online Interaction*, 161 UNIV. OF PENN. L. REV. 1579, 1587 (2019).

[480] Alan Z Rozenshtein, *Surveillance Intermediaries,* 70 STAN L. REV. 99, 122 (2019) ("**Alan Z Rozenshtein**").

[481] *In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court, No. 15-MC-1902(JO), 2016 WL 783565 (E.D.N.Y. Feb. 29, 2016) ("**Apple Inc. Warrant**").

[482] Special Rapporteur On The Promotion And Protection Of The Right To Freedom Of Opinion And Expression, UN Doc. A/HRC/29/32 (2015); *see also*, Jeffrey M Skopek, *Reasonable Expectations of Anonymity* 101 VA. L. REV. 691 (2015).

[483] Pratik Prakash Dixit, *Conceptualising Interaction between Cryptography and Law*, 11 NUJS L. REV. 327, 333 (2018). ("**Pratik Prakash Dixit**")

intermediaries, owners of the devices, or the person who possesses decryption key to carry out investigation.

Faced with this legal quagmire, the Supreme Court, has transferred several cases from High Courts across India, and is currently adjudicating upon the legal issue on whether the State can mandate the citizens to link their Aadhar cards to their social media accounts.[484] One of the cases from the Madras High Court involved determining a contentious issue as to whether WhatsApp can be mandated either by the government or judiciary to break the end-to-end encryption offered in its service, in pursuance of facilitating investigation on a case of child pornography.[485] Interestingly, two professors from Indian Institute of Technology, Madras, one of the premiere institutions for technical education in the country, gave contradicting expert evidence regarding whether WhatsApp has the ability to break the encryption.[486] While that question is outside the scope of this paper, this case is a clear demonstration of the government's desperation to use intermediaries for investigation purposes.

Digital evidence is merely evidence in digital form.[487] However, as Lex Gill in his seminal article has elucidated, the normative force of the metaphors used to describe cyberspace and big data and define privacy

---

[484] Facebook Inc. v. Union of India, T.P.(C) No. 1943-1946/2019, decided on 22.10.2019, https://main.sci.gov.in/supremecourt/2019/27178/27178_2019_15_8_17723_Order_22-Oct-2019.pdf.
[485] Facebook Inc. v. Union of India., 2019 (13) SCALE 13, ¶ 7.
[486] *Id.*
[487] Jenia I Turner, *Managing Digital Discovery in Criminal Cases,* 109 J. CRIM. L. & CRIMINOLOGY 237, 244 (2019).

within its contours has adverse legal consequences. The title of this paper borrows the phrase "metaphor problem" to highlight and acknowledge the cognitive gap in our conception of privacy in the digital age or cyberspace in juxtaposition to traditional and physical notions of privacy.[488] In order to demonstrate this, one could imagine a scenario where a police officer forcibly entering a person's house might not find out much about that person's personal life, preferences, habits and the like; in contradistinction, when the police officer searches a smartphone or the data provided by Internet Service Providers, they could obtain both relevant and irrelevant information on almost every aspect of the person's life. Therefore, traditional warrant requirement or warrant specification requirements might be seriously inadequate to protect the privacy of the individual.

Moreover, in a regular search and seizure of a residence the search precedes the evidence, *i.e.*, police sort out relevant and irrelevant objects immediately in the residence and procure the evidence solely required for the purposes of the trial. However, in cases of hard disks, computers or smartphones, the device is initially seized and then searched for evidence by performing cyber forensics.[489] In the process of searching, the irrelevant personal information of the target, or even third parties could be disclosed without the consent of the concerned person. For this reason, the author

---

[488] Lex Gill, *Law, Metaphor, and the Encrypted Machine*, 55(2) OSGOODE HALL L. J. 440, 454 (2018) ("**Lex Gill**").

[489] Paige Bartholomew, *Seize First, Search Later: The Hunt for Digital Evidence*, 30 TOURO L. R. 1027 (2014); *see also,* Swathi Mehta, *Cyber Forensics and Admissibility of Evidence,* PL JAN S-23, S-31 (2012) ("**Swathi Mehta**").

argues that specific warrants to digital locations within a device is necessary in case of digital searches.[490] In the context of procuring evidence from remote servers of third-party intermediaries, the servers contain massive amount of data which are not segregated person-wise thereby posing a greater risk of incidental encroachment into an individual's privacy without his/her consent or knowledge.[491]

In the Supreme Court's *K.S. Puttaswamy and Ors* v. *Union of India and Anr.*verdict [*hereinafter* "***Privacy Judgement***"],[492] the principle of proportionality was adopted, thereby, doing away with the "compelling state interest" test for encroaching into one's privacy. In this context, the substantive and procedural safeguards formed through conceptions of privacy in the physical space, if unquestioningly transposed to the digital space, it would drastically limit the constitutional protection afforded to privacy. Therefore, privacy in the digital space demands more apposite rules and procedural safeguards.[493]

This paper in Chapter II enumerates the different classifications of data that could be used in the course of an investigation. This classification would provide us with a proper understanding of the legal conundrums that digital searches had posed and could pose in the future. Chapter III explains

---

[490] James Saylor, *Computers as Castles: Preventing the Plain View Doctrine from Becoming a Vehicle for Overboard Digital Searches*, 79 FORDHAM L. REV. 2809 (2011).
[491] Sarit K Mizrahi, *The Dangers of Sharing Cloud Storage: The Privacy Violations Suffered by Innocent Cloud Users during the Course of Criminal Investigations in Canada and the United States,* 25 TUL. J. INT'L & COMP. L. 303, 319 (2017) ("**Sarit K Mizrahi**").
[492] *Privacy Judgement, supra* note 475, at ¶ 488.
[493] Orin S Kerr, *Digital Evidence and the New Criminal Procedure,* 105 COLUM. L. REV. 279, 306 (2005) ("**Orin S Kerr**").

the current law that governs the procurement of digital evidence in India emphasising on the overbroad and highly discretionary framework. It also traces the origins and causation of the framework back to the lack of a fundamental right to privacy or reasonable search and seizure. Chapter IV compares and deliberates on the ways in which the United States of America [*hereinafter* "**USA**"], Canada and the United Kingdom [*hereinafter* "**UK**"] have dealt with ensuring protection of privacy in digital search and seizures. This Chapter further attempts to highlight the significance of a constitutionally recognised fundamental right to reasonable search and seizure in these countries, in developing a data protection regime tilted more in favour of their citizens, unlike India. Lastly, Chapter V concludes by inculcating the lessons from the comparative study in the preceding chapters, enumerates vital points on which the framework of digital search and seizure in India needs to be transformed and modified to ensure protection to the citizen's privacy in the real sense.

II. IDENTIFYING CLASSIFICATION IN DATA: STORAGE, CONTENT AND PROTECTION

Understanding classifications in data based on their storage, content and protection would help us better appreciate the procedural and substantive laws that are used to harmonize the conflict between individual privacy and legitimate state interest in detecting crime, as discussed in the following chapters.

A. DATA AT REST AND DATA IN MOTION

Data which is stored in a particular device such as a smartphone, computer, laptop, or hard disk, including data which has been stored in remote servers by service providers are considered to be "data at rest".[494] On the other hand, "data in motion" is when the data in question is in motion or in transmission from one device to another,[495] and if wished to be accessed, it needs to be intercepted, *i.e.*, obstructed from reaching its destination or covertly observe the transmission without the knowledge of the person involved. For example, interception of telephone conversation means eavesdropping on calls, and interception of email communications or even text messages would mean that the message is routed through the police before it reaches the destination.

Here, Kerr explicates this type of classification by making a distinction between "retrospective" and "prospective" surveillance. While the former entails procuring the data or evidence that already exists in the form of digital storage; the latter involves procuring data that would be used for the purpose of investigation which is yet to come into existence.[496] This distinction becomes imperative because prospective surveillance denies the

---

[494] Pratik Prakash Dixit, *supra* note 483, at 332, 333.
[495] *Id.*
[496] Orin S Kerr, *supra* note 493*,* at 287.

subject of the investigation the "right to delete"[497] and therefore is more invasive.[498]

Unlike traditional services like telephones, it is more difficult to draw the line between prospective and retrospective surveillance in case of messaging services like Instagram and WhatsApp or other cloud service providers. It becomes essential for courts to determine this, since the procedural safeguards and threshold required to issue a warrant, are different for each type of data. Attempts made by courts in the USA and Canada in this regard are progressive and the same are discussed in Chapter IV below.

B. CONTENT AND NON-CONTENT INFORMATION

This classification, as the name suggests, depends on the information that is sought to be procured for the purpose of an investigation. The law enforcement might either need the actual contents of a particular communication, or only the information pertaining to the identity of the sender/receiver or location of the source of the communication.[499] For example, an email address, subscriber information shared with telecommunication providers, an IP address, are all

[497] COUNCIL REGULATION 2016/679 of April 27, 2016, PROTECTION OF NATURAL PERSONS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA, art. 17, 2016 O.L. (L 1191) 1; *see also,* Jorawer Singh Mundy v. Union of India, 2021 SCC OnLine Del 2306 (India).
[498] Patricia L Bellia, *The Memory Gap in Surveillance Law*, 75 U CHI. L. REV. 137, 161-166 (2008) at 176.
[499] Swathi Mehta, *supra* note 489, at ¶ 31.

characterized as "non-content information."[500] However, the actual contents of a telephone call, a text message or the body of an e-mail sent from one person to another, is considered to be "content information".[501] This kind of distinction seems to be relevant when law enforcement approaches third parties for information on their customers, instead of directly conducting a search and seizure of the subject of the investigation. Clearly, when law enforcement authorities could directly seek and obtain content-information from third parties, it is more intrusive than when non-content information is sought for.

Even procedural safeguards in obtaining the same would differ, for example while non-content information could be procured from third party without the consent of the end customer, or it could even be argued that such consent need not be obtained, but the same could not be the case for contents of particular communications of the customer.[502] This distinction further grants the warrant granting authority an opportunity to minimise the data that is to be procured by the law enforcement.[503]

---

[500] Mathew J. Tokson, *The Content/Envelope Distinction in Internet Law,* 50.6 Will. & Mary L. Rev. 2105, 2113-2116 (2009).
[501] Orin S Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN L. R. 1005, 1019 (2010).
[502] Dan Jerker & Lodewijk Van Zweisston, *Law Enforcement Access to Evidence via Direct Contact with Cloud Providers- identifying the Contours of a Solution,* 32 COMP. L. & SEC. REV. 671, 679 (2016).
[503] *Id.*

C. ENCRYPTED DATA

Given that a lot of personal information is stored in devices and remote servers, and further considering the prominence of social media in today's world, any consumer would wish to protect their personal information. Encryption offers that protection by transforming plaintext into unintelligible form either by way of one-way (impossible to recover) or two-way encryption.[504] The purpose of it is to make the data unreadable to anyone other than the person who has the decryption key.[505]

Generally, arguments against encryption or for diluting encryption presuppose a privacy-security trade-off,[506] where the privacy of an individual is sacrificed for the security of another/ the greater good. However, it is a bit parochial to suggest that encryption disregards security interests since encryption offers protection to the data of any person available in any electronic device/storage device. Therefore, the contradictions of encryption and security are better understood only as a security-security trade-off, *i.e.*, the security of one individual is compromised for the security of another.[507] This is precisely the reason why the Encryption Policy, 2015, that was proposed by the Indian government (now withdrawn) and provided for overreaching investigatory powers to the state, prohibitive data retention requirements and also for a centralised

---

[504] Information Technology (Certifying Authorities) Rules, 2000, Schedule V.
[505] Orin S Kerr & Bruce Schneier, *Encryption Workarounds,* 106 GEO L. J. 989, 994 (2018) ("**Kerr & Schneier**").
[506] Alan Z Rozenshtein, *supra* note 480, at 137
[507] *Id.*

decryption key in control of the government,[508] was vehemently opposed by the intermediaries and general public.

There are broadly two types of encryptions currently used by service providers. The first type is where the encryption key cannot directly be used by the consumers such as in services like email, ATM machines, smartphones or other devices. [509] The end user of the product or service is likely to create a password or a passcode which in turn decrypts the decryption key in the first instance, followed by the key decrypting the content.[510] This could be further classified into symmetric and asymmetric encryption. This distinction, however, is not necessary since symmetric encryption is outdated, and currently due to the advantages in its application, only asymmetric encryption is used in almost all e-commerce and internet services.[511] Asymmetric encryption entails a "public key known to all persons" and a "private key" which is only used by recipient to decrypt the messages, essentially enabling random but secure transactions and interactions in cyberspace.[512]

The second type of encryption can be seen in services that employ end-to-end encryption, wherein the process of decryption is "practically invisible to the consumer".[513] This kind of encryption has gained a lot of

---

[508] Bedavyasa Mohanty, *supra* note 478, at 4 -7.
[509] Pratik Prakash Dixit, *supra* note 483, at 330.
[510] *Id.*
[511] *Id.* at 331.
[512] *Id.*
[513] Kerr & Schneier, *supra* note 505.

traction in messaging services such as WhatsApp, Signal and Telegram. The primary goal of end-to-end encryption is to ensure the consumers their privacy and sometimes particularly anonymity.[514] Unlike asymmetric encryption, in the case of end-to-end encryption, even the service provider do not possess the keys required to decrypt content, which makes it practically impossible for them to provide the key to a government agency.

Encryption techniques leave the law enforcement's hands tied. This means that they need to depend either on the owner of the personal devices or third-party intermediaries for passwords/decryption. In the former, the right against self-incrimination[515] is triggered when the police or courts are trying to obtain the data by forcing the accused/owner of the personal device to provide the password. The latter gives rise to a host of issues ranging from, the extent to which a third-party intermediary is required to divulge personal information of the customer to the procedural safeguards for law enforcement to obtain encrypted information.

III. INDIAN LAW ON PROCURING DIGITAL EVIDENCE

There are very few judgements discussing the direct conflict between search and seizure and an individual's right to privacy in India. The Supreme Court in *M. P. Sharma v. Satish Chandra*[516] had defined search and seizure as an "overriding right" of the State in the interest of security. In the Supreme Court's opinion, restricting security interests by reading in

[514] Alan Z Rozenshtein, *supra* note 480, at 137.
[515] INDIA CONST., art. 20 cl. 3.
[516] M. P. Sharma v. Satish Chandra, AIR 1954 SC 300 ("***M. P. Sharma***").

right to privacy would be contrary to the intention of the framers of the Constitution of India [*hereinafter* "**the Constitution**"], specifically emphasizing that our Constitution lacks provisions similar to 4th Amendment in the USA or Section 8 in the Charter of Bill of Rights in Canada.[517] Only much later in *Gobind v. State of Madhya Pradesh*[518] did the Supreme Court indicate that a "compelling state interest" can legitimately encroach upon a person's fundamental right to privacy (recognised under Article 21 of the Constitution). Except for recognizing that detecting crime is a legitimate state interest,[519] the Supreme Court in overruling *Gobind v. State of Madhya Pradesh* in the *Privacy Judgement* had not dealt with the contradictions between an individual's right to privacy, and the scope of the law enforcement's power in case of a search or seizure. Clearly, the privacy jurisprudence in India is in its nascent stages. No attempt has been made by the legislature to reconsider the existing provisions for search and seizure, and the surveillance power of government in the light of the *Privacy Judgement*.

A. DATA AT REST

The provisions of the Criminal Procedural Code, 1973 [*hereinafter* "**CrPC**"] in respect of search and seizure appears to be the only law applicable in respect of procurement of data at rest.[520] According to this law, for any 'place' to be searched a general search warrant is required.[521]

---

[517] *Id.* at ¶ 20.
[518] Gobind v. State of Madhya Pradesh, 2 SCC 148 (1975), ¶¶ 24,28.
[519] *Privacy Judgement, supra* note 475, at 484.
[520] CODE CRIM. PROC., §93.
[521] *Id.*

The warrant shall be granted if the Magistrate "has reason to believe" that it is necessary for investigation or trial. However, there are no specific additional requirements prescribed for a police officer to minimize the scope of the search, if such search is undertaken on an electronic device. Though, the Magistrate has the discretion to add more specifications to the warrant restricting the scope of the search, there have been no cases where it has been used for electronic devices.[522]

In India, the police have a large scope to circumvent these warrant requirements as they have the powers to obtain the device without judicial oversight. The police also have the discretion to issue a written order mandating a person to produce a document or a thing.[523] There is also no burden on the police officer or the magistrate issuing summons to adjudicate, or pass the muster of a probable cause or a reasonable ground threshold; the written order can be issued solely on the basis of whether the officer feels it is "necessary or desirable".[524] The police officer has the discretion to search any place in his jurisdiction without a warrant and all that the officer needs for justifying the same is merely his "opinion" that such procedure would cause "undue delay" in the investigation.[525] This insubstantial framework is further devitalised by the courts in India which have also rejected the "fruit of the poisoned tree" doctrine[526] (which renders

[522] CODE CRIM. PROC., §93(2).
[523] CODE CRIM. PROC., §91.
[524] *Id.*
[525] CODE CRIM. PROC., §165.
[526] Silverthorne Lumber Co. v. United States, 251 U.S. 385 (1920).

any evidence to be inadmissible in court, if it has been obtained by illegal means, not following due process of law), and has held that the evidence collected without the authority of law is not illegal or inadmissible in court of law but merely a procedural irregularity.[527]

The Information Technology Act, 2000 [*hereinafter* "**IT Act**"] applies where data has to be obtained from ISPs or social media service providers. The primary objective of the IT Act was to legitimise the use of digital signatures and also provide a comprehensive framework to preserve its authenticity.[528] Unless in circumstances provided under the Act or any other law, an intermediary is prohibited from disclosing any person's personal information.[529] However, the IT Act does not have a provision which explicitly authorises a government agency or police officer to collect information from a third party.

The safe harbour provision of the IT Act which exempts intermediaries from liability mentions that the intermediary is bound to observe "due diligence" or any other guidelines as prescribed by the Central Government.[530] The due diligence required by the Central Government does not provide for any *ex ante* judicial supervision on the process of procuring data from intermediaries, but mandates that the intermediary

---

[527] Pooran Mal v. Director of Inspection AIR 1974 SC 348, ¶ 34; *see also,* State of Maharashtra v. Natwarlal Damodardas Soni, AIR 1980 SC 593, ¶ 9; Radhakrishnan v. State of UP, 1963 Supp. 1 S.C.R. 408.

[528] Shruti Chaganti, *Information Technology Act: Danger of Violation of Civil Rights*, 38 EPW WEEKLY 3587-3595 (August 23-29, 2003).

[529] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000, § 72A.

[530] *Id.* at §79(c).

shall provide the data within 72 hours of an order in writing, stating the reasons for such a request by a *"Government agency lawfully authorised for investigative or protective or cyber security activities"*.[531] Intermediaries also comply with such requests to prevent any unnecessary liability because assistance in such a manner is not regarded as an invasion to privacy in this legal framework, but a form of due diligence that the intermediary is bound to follow to prevent any kind of penalty.[532]

The encryption of personal devices poses yet another conundrum. In this case, the law enforcement needs to depend on the subject of the investigation to procure the data itself. If the personal devices are locked due to encryption by the subject, then there is a possibility that the law enforcement will force the subject to provide the password. In case, the devices are locked using a finger print, the bar under Article 20(3) of the Constitution will not operate because the Supreme Court in *State of Bombay v. Kathi Kalu Oghad* [*hereinafter "**Kathi Kalu**"*] held that finger prints, retinas, handwriting or signature samples even though amount to furnishing evidence, concealing the same cannot "change its intrinsic character" and therefore will not amount to "being a witness" against himself.[533] The concurring judgement of Justice Das Gupta (speaking for Justices Sarkar and S.K. Das) took a contrary view of the phrase "to be a witness" in Article 20(3) and held that it includes providing documentary evidence under

---

[531] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r.3(j).
[532] *Id.* r.7.
[533] State of Bombay v. Kathi Kalu Oghad, AIR 1961 SC 1808, ¶ 12 ("***Kathi Kalu***").

compulsion, whereas the majority judgement of Chief Justice B.P. Sinha specifically excluded them and restricted the scope only to furnishing testimonial evidence.[534]

There has been a considerable shift in interpreting the right against self-incrimination. While *Kathi Kalu* relied heavily on the nature of evidence, *Selvi v. State of Karnataka*[535] [*hereinafter* "***Selvi***"] seems to have placed more emphasis on the personal autonomy and right of the accused/subject to reveal his information.[536] It was held in *Selvi* that Article 21 and 20(3) of the Constitution are interrelated and essentially conceptualised self-incrimination in terms of personal autonomy and control that a subject has over what information they could divulge during an investigation.[537] However, its applicability to data within personal gadgets already confiscated is questionable because the Supreme Court was only dealing with whether the evidence in question is testimonial or material in nature.[538] Digital evidence falls under "documentary" evidence,[539] and the same is outside the scope of Article 20(3) unless the document in question is a confession obtained through coercion as per the ratio of *Kathi Kalu*.[540] Furthermore, it is interesting to note that even though the opinion of Justice

---

[534] *Id.* at ¶ 13.
[535] Selvi v. State of Karnataka, AIR 2010 SC 1974 ("***Selvi***").
[536] *See generally,* Aditya Sarmah, *Privacy and Right against Self-incrimination: Theorising a criminal process in the Context of Personal Gadgets*, 3 CONST. AND ADMIN. L. QUAT. 30 (2017) ("**Aditya Sarmah**").
[537] *Selvi*, *supra* note 535, at ¶ 191-193.
[538] *Id.* at ¶ 129.
[539] Evidence Act, 1872, §3.
[540] *Kathi Kalu*, *supra* note 532.

Das Gupta in *Kathi Kalu* held that the words "to be a witness" included documentary evidence,[541] it managed to concur with the majority. Justice Das Gupta, interpreting the words 'against himself', held that since providing his fingerprint was only for the purpose of comparison with the document already in possession of the police, it would not amount to self-incrimination as he is not directly providing evidence against himself.[542] Following *Kathi Kalu* and *Privacy Judgement*, the Karnataka High Court very recently issued guidelines for procuring electronic evidence which specifically states that forcing a witness to provide password or fingerprint is not barred by Article 20(3) and that the investigation officer is within his power to require a citizen or an intermediary to decrypt any information.[543]

B. DATA IN MOTION

It is important to understand the development of the interception of "telegraphic communications"[544] in order to critically examine the current provisions pertaining to interception of electronic communications under the IT Act. The limitations placed for the purpose of interception of telegraphic communications was based on restrictions to free speech from Article 19(2) of the Constitution (excluding defamation).[545] This clearly defines the purpose for which such interception shall be made and the same was also subject to judicial review (this review is only *ex post* surveillance),

---

[541] *Id.* at ¶ 27-33.
[542] *Id.* at ¶ 36-37.
[543] Virendra Khanna v. State of Karnataka, MANU/KA/0728/2021, ¶ 12.25, 12.26 & 15.
[544] The Telegraph Act, 1885, § 3(1).
[545] Bedavyasa Mohanty, *Inside the machine Constitutionality of India's surveillance apparatus*, 12 IND. JOUR. LT 206, 212 (2016).

unlike the previous version where interception is justified by proving "public emergency" or "public safety", the existence of which is to be wholly determined by the Executive.[546]

While almost replicating the provision in the Telegraph Act, the additional words "for any other investigation"[547] in the IT Act enables any agency authorised by state or Central government, or officers authorised by either of them, to intercept electronic communications for any purpose. The intermediaries would face criminal charges if technical assistance or any other facilities under Section 69(3) of the IT Act is not provided.[548] This deviation from the purpose limitation that exists in the Telegraph Act is completely unfounded and unsubstantiated.

Moreover, scope of "assistance" by an intermediary is very vaguely worded and could encompass all types of assistance including decrypting content information for the purpose of investigation without the knowledge of the customer. The assistance requirement not only includes interception, but also extends to decryption and the intermediary is exempted from the criminal liability only when it is practically impossible for them to decrypt it.[549] It is to be noted that decryption orders under the said rules extends to both, data in rest and data in motion.

---

[546] *Id.*
[547] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000, §69.
[548] *Id.* at §69(4).
[549] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, r.17 ("**Interception Rules**").

It is clearly noticeable that there is absolutely no attempt by the legislature to classify data as elaborated in Chapter II, to specifically provide procedures for each of them. On the contrary, the provision enabling interception, monitoring and decryption is merely a blanket power in the hands of police. The procedural safeguards that are notified by the Central government[550] do not provide for any warrant or prior judicial authorisation for the police to intercept electronic communications.[551] The entire process from the grant of approval[552] to the periodic review of the approvals[553] rests with the executive.

The procedural safeguards in the IT Act for interception was also a mere replication of the guidelines issued in the case of *People's Union for Civil Liberties (PUCL)* v. *Union of India* [*hereinafter* "***PUCL***"].[554] While the powers to intercept telegraphic communications was challenged, the Supreme Court formulated guidelines in *PUCL*[555] which was later codified in the Telegraph Rules.[556] In framing the guidelines the Supreme Court specifically refrained from providing for a prior judicial authorisation since it would not be within the scope of the principal legislation.[557] In merely replicating these guidelines and also diluting the purpose limitation existing in the

---

[550] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000, §69.
[551] Interception Rules, *supra* note 531, at r.3.
[552] *Id.*
[553] *Id.* at r. 2(q)
[554] *See Generally*, Vishal Kanade, *Tap-Tap Who is Listening-Prying into Privacy*, 5 L. REV. GLC 171 (2006).
[555] People's Union for Civil Liberties v. Union of India, 1 SCC 301 (1997) ("***PUCL***")
[556] The Telegraph Rules, 1951, r.419A.
[557] *PUCL*, *supra* note 555, at ¶ 34.

Telegraph Act, the legislature has significantly reduced the scope of protection to its privacy. The principles and procedures propounded in *PUCL* are also very outdated and even though it is in the context of mass surveillance, in light of recent developments in technology and the privacy jurisprudence in India, it needs to be revisited.[558] These procedures currently lack any mandate as to interception/intrusion into one's privacy being the least restrictive measure among other possibilities, lacks any specific tailored procedures for each type of data, are over broad provisions and does not take into account the severity of the offence. It is apparent that the Telegraph Rules do not pass the muster of proportionality test as propounded in the *Privacy Judgement*. Currently, more than ten agencies are authorised by the Central government to demand information of any kind on citizens that is in possession of third-party intermediaries.[559]

India has always preferred the "Crime Control Model" over the "Due Process Model", placing more emphasis on "eliminating crime" than individual liberties of the accused.[560] It can be gleaned from the legal framework for procuring digital evidence in India that there is no effort to balance the competing interests of the State and the individual. There is no law legitimising the power of law enforcement to mandate information from third party service providers, but the power itself is defined in terms

---

[558] Chaitanya Ramachandran, *PUCL v. Union of India Revisited: Why India's Surveillance Law must be Redesigned for the Digital Age,* 7 NUJS L. Rev. 105 (2014).
[559] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000, § 69; Ministry of Home Affairs, Order S.O. 6227(E) dated December 20, 2018, http://egazette.nic.in /WriteReadData/2018/194066.pdf.
[560] Aditya Sarmah, *supra* note 536, at 39.

of obligations that the intermediaries are bound to follow to prevent getting wounded up in any criminal proceedings instituted against them. The Intermediary Guidelines place further burden on the intermediaries such as mandating them to enable tracing of individuals[561] and also require them to proactively determine and remove unlawful content,[562] which in essence amounts to privatising law enforcement.

IV. PROCURING DIGITAL EVIDENCE IN OTHER JURISDICTIONS

This chapter looks at the negative obligation of the state not to intrude into an individual's privacy, as it exists in the USA, Canada and the UK in terms of digital evidence. These countries were chosen as they were extensively discussed in the *Privacy Judgement* while recognising informational privacy. This comparison is done solely for the purpose of understanding the intricacies and predicaments that the courts have struggled with and also how the "metaphor problem" has been addressed or overcome in these jurisdictions. Even though, these regimes are not ideal and are still evolving, in juxtaposition to India they appear to be much more mature in terms of procedural due process.

A. UNITED STATES OF AMERICA

The framework developed in USA can be characterized as a patchy work, developed sporadically over a period of time, as and when the digital

[561] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 3(j).
[562] *Id.,* r. 4(4).

market demanded such laws, and is often criticised for the same reason.[563] Procurement of digital evidence is considered to be a Fourth Amendment Search under the US Constitution and therefore all the principles of reasonable search and seizure apply automatically.[564] Given the high regard for privacy rights given in the USA post-independence, it seems incredibly difficult to translate them into the context of digital evidence[565] and in that process, some compromises have been made.

i. Warrant, but Only for 180 Days

The Stored Communications Act, 1986, distinguishes between an Electronic Communication Service [*hereinafter* "**ECS**"] provider and a Remote Computing Service [*hereinafter* "**RCS**"] provider, for the purpose of allowing any government entity to procure data from a third party.[566] While the former can be messaging services like WhatsApp, Facebook Messenger or email services, the latter comprises of services provided only for the purpose of storage "on behalf" of the consumer.[567] The ECS and RCS providers aren't mutually exclusive and most of the times the services overlap. For example, social media websites provide communication services and also act as RCS providers.[568] It is pertinent to note that unlike

---

563 Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, Fourth Amendment, and Statutory Law Enforcement Exemptions,* 111 MICH. L. R. 485, 495 (2013).
564 Orin S Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 564 (2005) ("**Kerr**").
565 *See generally,* Donald A Dripps, *Dearest Property: Digital Evidence and the History of Private Papers as Special Objects of Search and Seizure,* 103 J. CRIM. L. & CRIMINOLOGY 49 (2013).
566 18 U.S.C §2703 (1976).
567 *Id.* at § 2711(2).
568 Crispin v. Christian Audigier, Inc. 717 F. Supp. 2d 965 (C.D. Cal. 2010).

the classifications mentioned in Chapter II, this distinguishes between the types of service that a third party provides the user.

Apart from defining ECS in terms of type of service, the Act prescribes an arbitrary cut-off date of 180 days, within which the government is mandated to get a warrant from a court of competent jurisdiction to procure data from ECS providers.[569] However, after 180 days, the law deems that the storage of such communication is not for providing any communication services such as emails or messages, but the service provider only acts as an entity providing storage for the user. Hence, after 180 days, a subpoena, as applicable to an RCS provider, is enough to mandate the intermediary to provide the content information provided prior notice is given to the consumer.[570] If the government entity doesn't want to provide notice it has to either opt for a warrant[571] or a get judicial authorisation for a delayed notice.[572]

This warrant requirement flows from the Fourth Amendment, which mandates that for the citizen shall not be subject to "unreasonable search and seizure" and therefore the judge would have to be satisfied that there is "probable cause" for a warrant to be granted.[573] Usually, the law

---

[569] 18 U.S.C §2703(a) (1976).
[570] *Id.* at 2703(b).
[571] *Id.*
[572] 18 U.S.C §2705 (1976).
[573] Reema Shah, *Law Enforcement and Data Privacy: A forward Looking Approach,* 125 YALE L. J. 543, 545 (2015).

enforcement waits for 180 days since the RCS requirements are relatively less stringent than the ECS requirements.[574]

Furthermore, the lower courts have also distinguished between opened and unopened communications stating the reason that when a message or email is opened within 180 days, then the ECS provisions ceases to apply because once the communication has reached the destination, the service provider only stores the same on behalf of the consumer and therefore acts as an RCS provider.[575] The Supreme Court of the United States [*hereinafter* "**SCOTUS**"] also emphasised the differential expectation of a citizen's privacy in case of content and non-content information.[576] Any non-content information from an ECS or an RCS provider can also be done only through a court order.[577] Even though the 180 days cut-off seems arbitrary, the mandatory warrant requirement and the explicit consent requirement, seems to provide sufficient judicial oversight prior to procuring the personal data.

ii. Acknowledgment of the Metaphor Problem by the Judiciary

The US jurisprudence had formulated the "third party" doctrine, which negates the existence of a reasonable expectation of privacy if

---

[574] Sarit K Mizrahi, *supra* note 491*,* at 333.
[575] Christopher J. Borchet et al., *Reasonable Expectations of Privacy Settings: Social Media and the Stored Communications Act,* 13 DUKE L. & TECH REV. 36, 49 (2015).
[576] Sarah Wilson, *Compelling Passwords from Third Parties: Why the Fourth and Fifth Amendments Do Not Adequately Protect Individuals when Third Parties Are Forced to Hand Over Passwords*, 30 BERKLEY TECH. L. J. 1, 17(2015) ("**Sarah Wilson**").
[577] 18 U.S.C §2703(c) (1976).

information is voluntarily disclosed to a third party.[578] Contrary to that, in cases of cell phones 'cell site location data", the SCOTUS held that in this digital age all data shared to intermediaries could not possibly be a voluntary affirmative action on part of the customer that negates the legitimate expectation of privacy.[579] In yet another instance, the SCOTUS held that compelling production of emails from ISPs without warrant is unconstitutional irrespective of it being a third party.[580] Similar to this departure from the third party doctrine, the SCOTUS in the context of frisking and searching a person, held that unlike normal documents of a person, a cell phone differs *"qualitatively and quantitatively"* and has the potential to disclose almost every personal information of any citizen and therefore, a warrant is required for searching the same.[581]

The Federal Rules of Criminal Procedure also recognise the two-step process involving seizing and searching of personal devices and data storage devices and allows copying of data on site.[582] The results of this overt emphasis on the metaphor problem by the SCOTUS is clearly reflected in the recent trend of magistrates across the USA including minimisation requirements in their warrants, essentially issuing protocols providing for minimal and only necessary data to be accessed to ensure that

[578] Katz v. United States, 389 US 347 (1967).
[579] Carpenter v. United States 138 S.Ct. 2206 (2018), ¶ 18-22.
[580] United States v. Warshak, 631 F.3d 266 (6th Cir. 2010)
[581] Riley v. California, 573 U.S.373 (2014), ¶ 17-21.
[582] Fed. R. Crim. P. 45(a)(e)(2).

the informational privacy of their citizens is protected.[583] Even though it is not considered a constitutional requirement,[584] the warrant for search of an electronic device was accompanied with protocols to restrict the data that is procured; for example, a mandatory condition restricting the search to data with ".jpg" (picture) file extension.[585] Clearly, with lack of any guidance and affirmative pronouncement of the Indian judiciary on the metaphor problem, unlike USA, the lower courts in India find absolutely no use for minimisation requirements.

iii. The Hurdles Surrounding Interception

While the Wiretap Act[586] regulated the process of intercepting telephone communications, the Electronic Communications Privacy Act, 1986[587] amended these provisions to make them compatible with electronic communications.[588] In case of interception of electronic communications, a prior authorisation of the application must be granted by the Attorney General in case of an application to a Federal Court judge, and principal prosecuting attorney in case of a State Court judge.[589] The offences for which an authorisation could be provided, is exhaustively enlisted in the legislation which means that the purpose for which law enforcement could

---

583 *See Generally,* Emily Berman, *Digital Searches, the Fourth Amendment, and the Magistrates 'Revolt',* 68 EMORY L J 82(2018).
584 *United States v. Comprehensive Drug Testing, Inc.,* 513 F.3d 1085 (9th Cir. 2008).
585 *United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999).
586 Title III, Omnibus Crime Control and Safe Streets Act, 1968 (Wiretap Act).
587 18 U.S.C §2510-2522 (1976).
588 Sarah Wilson, *supra* note 102, at 31.
589 18 U.S.C §2516 (1976).

invoke this power is restricted.[590] The court must be satisfied of probable cause of the offence itself and the probable cause of the interception providing evidence. Furthermore, the court must also be satisfied of the complete exhaustion of other investigative methods or confirm that they "reasonably appear unlikely to succeed".[591] A judge of competent jurisdiction, in case of interception does not include magistrates unless the statute specifically provides for the same, but only includes a district or court of appeals judge.[592]

Communications Assistance for Law Enforcement Act, 1994 [*hereinafter* "**CALEA**"] is primarily a law mandating assistance to law enforcement for the purpose of wiretapping and it applies only to "telecommunications carriers".[593] Compliance with substantive provisions in CALEA would be necessary for facilitating a wiretap, and as a consequence the judge passing the court order is also given the power to enforce the same.[594] However, contrary to popular belief these provisions do not apply to electronic communication services and do not address encryption in any manner.[595] The Federal Communications Committee [*hereinafter* "**FCC**"], is given the power to expand the scope of the CALEA and deem any service that replaces the local telephone exchange services as

---

[590] *Id.*
[591] *Id.* at 2518(3).
[592] *Id.* at 2510(9).
[593] Justin (Gus) Hurwitz, *Encryption Congress Mod (Apple + CALEA),* 30 HARV. J. L. & TECH. 355, 376 (2016) [*hereinafter*, "**Justin (Gus) Hurwitz**").
[594] 18 U.S.C §.2522 (1976).
[595] Justin (Gus) Hurwitz*, supra* note 593, at 382.

a "telecommunication carrier", but there is still an ambiguity as to whether it could apply to WhatsApp and email services which primarily provide the specifically exempted "information services" under the CALEA.[596] This differential approach towards "interception" is because it is more intrusive than procuring data at rest. Not only prior judicial authorisation in terms of warrant is required, but a District or Appeals Judge is required to be satisfied that interception is the last possible tactic to procure information and prosecute the offenders.[597]

iv. Encryption and the Silent Spectator

With respect to encryption, the legal framework in the USA remains silent. While it authorises government entities to procure data from third parties, there is no mandatory requirement for the third party to provide the decryption key. While the FBI cited that the courts still had the power to mandate the intermediary, in a case involving Apple Inc. under the All Writs Act,[598] the Court rejected the argument and held it had no obligation to decrypt the phone.[599] While in the late 1990s it was argued that courts were not very keen on including rights beyond the text of the US Constitution,[600] clearly courts now have realised that due process requirements under the Constitution need to be self-tailored to adapt to the new implications of digital evidence on the right of privacy. However, the

---

[596] *Id.* at 387.
[597] 18 U.S.C § 2518(3)(c) (1976).
[598] 28 U.S.C § 1651 (2012).
[599] Apple Inc. Warrant, *supra* note 481.
[600] *See Generally,* Zhonette M Vedder-Brown, *Government Regulation of Encryption: The Entry of Big Brother or the Status Quo* 35 AM. CRIM. L. REV. 1387(1998).

protection offered by a mandatory key disclosure law, if passed, would heavily depend upon the kind of metaphor that the courts choose to apply to an encrypted information.[601]

The police could also compel the owner of a personal gadget to decrypt a message. In case of providing a fingerprint, just like *Kathi Kalu* in India, the courts in USA could justify the same by citing *State v. Doe*[602] which came to a similar conclusion, *i.e.*, compelling to produce fingerprints wouldn't amount to incrimination and is not hit by the Fifth Amendment. While compelling to produce documentary evidence including digital evidence, does not necessarily attract the Fifth Amendment, unlike India, the US courts have developed an exception called the act-of-production testimony, *i.e.*, the act of producing the document by itself is testimonial in nature and incriminates the citizen.[603] Interestingly the exception to that application is the presence of a foregone conclusion which means that the police were already aware of this knowledge or the contents of the documents, and in that case it would not be deemed testimonial.[604] *Commonwealth v. Dennis Jones*[605] is the only case that clearly sets out the law on compelling decryption of personal devices, and the Court held that the Fifth Amendment protection extends only to testimonial acts, and the law

---

[601] A Michael Froomkin, *Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution,* 143 U PA L. REV. 709, 884 (1995).
[602] State v. Doe, 465 U.S 605.
[603] Laurent Sacharoff, *Unlocking the Fifth Amendment: Passwords and Encrypted Devices,* 87 FORDHAM L. REV. 203, 219 (2018).
[604] *Id.*
[605] Commonwealth v. Dennis Jones, 117 N.E.3d 702 (Mass. 2019).

enforcement can compel a person to provide their password if it is proved "beyond reasonable doubt" that the defendant knows the password.[606] However, it is unclear as to how the subject's right against self-incrimination and forced testimony could be influenced by his knowledge of the device's password.

B. CANADA

Similar to the Fourth Amendment to the US Constitution, Section 8 of the Charter of Rights of Canada,[607] protects citizens from unreasonable search and seizure. The Supreme Court of Canada [*hereinafter* "**Canadian SC**"] laid down the pre-requisites for a valid search namely pre-authorisation by a neutral body,[608] authorised by a reasonable law and reasonableness in the search itself.[609] A reasonable expectation of privacy is a prerequisite for a particular search to fall under Section 8, and consequentially such search to be subject to various constitutionally guaranteed procedural and substantive safeguards.[610] The provisions regarding procuring digital evidence are encapsulated in the Criminal Procedure Code of Canada.

---

606 David Rassoul Rangaviz, *Compelled Decryption & State Constitutional Protection against Self-Incrimination,* 57 AM. CRIM. L. REV. 157,158 (2020).
607 Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, being Schedule B to the Canada Act, 1982 (U.K), 1982, c. 11.
608 Hunter v. Southham, [1984] 2 S.C.R 145.
609 Lee Ann Conrod, *Smart Devices in Criminal Investigations: How Section 8 of the Canadian Charter of Rights and Freedoms Can Better Protect Privacy in the Search of Technology and Seizure of Information,* 54 APPEAL 115, 121(2019) ("**Lee**").
610 *Id.*

i. Data at Rest: Subjective Judiciary and an Equivocal Parliament

The general search warrant[611] is the most commonly used provision to seize and search devices, and storage drives of the subject. In the context of a general search warrant as regards personal electronic devices like computers or laptops, the Canadian SC[612] rightly addressed the metaphor problem. It held that receptacles as understood previously cannot be applied to these devices, and specific prior judicial authorisation was absolutely necessary to seize and search these devices.[613] While warrantless searches are usually allowed in case of search incident to arrest, the Canadian SC[614] held that personal devices such as smartphones are capable of having varying degrees of personal information and hence could not be equated to a purse or a briefcase.[615] However, in both the cases a specific protocol to search or a minimisation requirement within the warrant was not considered constitutionally necessary.[616] Furthermore, the Canadian SC also specifically refrained from formulating particular tests and also pinning the level of protection offered to a citizen to the level of protection offered by technology itself.[617] For example, it cannot be argued that merely because

---

611 Criminal Code, R.S.C, (1985) c. C-46, §487.01 ("**Criminal Code**").
612 R v. Vu, [2013] 3 SCR 657.
613 *Id.* at ¶¶ 49,50.
614 R v. Fearon [2014] SCR 621.
615 *Id.* at ¶¶ 180-183.
616 Susan Magotiaux, *Out of Sync: Section 8 and Technological Advancement in Supreme Court Jurisprudence,* 71 SC L. REV.: OSGOODES ANN. CONST. CC 501, 508 (2015) ("**Susan**").
617 *Id.*

a citizen does not have an encryption to his smartphone there exists no reasonable expectation to privacy.

In case of procuring data from third parties like ISPs and Online Content Service [*hereinafter* "**OCS**"] providers, the framework consists of different types of production orders namely general production order,[618] production of transmission data,[619] tracing a particular communication,[620] tracking data[621] and even financial data.[622] The judge deciding a case, would have to be satisfied that such data would aid in the investigation of any offence.[623] Similar to the USA, information as to identity or non-content information are considered to be outside the scope of privacy.[624] This is also reflected in the different thresholds specified, such as "reasonable grounds to believe" for a general production order, and "reasonable grounds to suspect" for orders involving transmission of data, or specific communications.

The Canadian SC, emphasising on anonymity, has recently held that even basic subscriber information collected from ISPs are of a nature that it could reveal the intrinsically personal information which the subscriber wishes to keep a secret or remain anonymous, and the same would be

---

618 Criminal Code, R.S.C, (1985) c. C-46, §487.014.
619 *Id.*, at §487.016.
620 *Id.*, at §487.015.
621 *Id.*, at §487.017.
622 *Id.*, at §487.018.
623 *Id.*, at §487.015.
624 R v. Plant, [1993] 3 S.C.R 281; *See* R v. Spencer, (n.127).

reasonable only if there is prior judicial authorisation.[625] The Canadian SC has also acknowledged that a person could have reasonable expectation of privacy over a text message sent by him/her, stored in the device of some other person.[626] The courts have consistently refrained from formulating any rigid tests, and prefer to decide them on a case to case basis, probably to prevent the derailment of an evolving privacy jurisprudence.[627] However, in spite of rejecting the third-party doctrine, the courts have found a way to circumvent the lack of access to the data by including the contracts between the service providers and customers as an important criterion to decide whether there is a reasonable expectation of privacy.[628]

In pursuance of a conscious effort to retain the flexibility of Section 8 jurisprudence, courts in Canada have formulated several caveats[629] that have resulted in ambiguity in applying the law. Additionally, the Criminal Procedure Code of Canada also exempts every entity from any kind of liability as to voluntarily disclosing information to the law enforcement for the purpose of an investigation without the consent of the service provider.[630] This obliqueness has provided enough ambiguity and leeway for the law enforcement to circumvent warrants and obtain data from third parties to aid their investigations.[631] Even recently, Protecting Canadians

[625] R v. Spencer, 2014 SCC 43, ¶¶ 38, 68.
[626] R v. Marakah, 2017 SCC 59.
[627] Lee, *supra* note 609, at 115-117.
[628] Sarit K Mizrahi, *supra* note 491, at 328.
[629] Lee, *supra* note 609, at 124.
[630] Criminal Code, R.S.C, (1985) c. C-46, §487.0195.
[631] Sarit K Mizrahi, *supra* note 491, at 125.

from Online Crimes Act, 2014[632] was enacted hastily as a reaction to a tragic case of cyber bullying, and has caused to overlook privacy implications by significantly increasing the scope for law enforcement to request data from intermediaries.[633] Even though the higher level judiciary attempts to address the metaphor problem, the Canadian Parliament on the other hand is equivocal and ambiguous with regard to its purpose and intent.

ii. Finding an Investigative Necessity for Data in Motion

In case of interception, the law attempts to place procedural safeguards that are proportional to the intrusiveness of a Section 8 search.[634] To intercept, additional to the requirements of a general warrant, the law enforcement must convince the judge that there is an investigative necessity to conduct such an interception. The law enforcement agencies either have to prove that other methods have been exhausted or are unlikely to succeed, or that they are impractical given the urgency of the matter.[635] It has been clarified by the Canadian SC that the investigative necessity need not always be the last resort but there is burden on the police to present an affidavit with all facts and circumstances concisely to make sure there are "reasonable and probable grounds" to believe such interception is necessary and legal.[636] These additional requirements do not however, apply to investigations on terrorist activities or investigations into criminal

---

[632] Protecting Canadians from Online Crimes Act, 2014, S.C. 2014, C-31.
[633] Robert Diab, *The Road Not Taken: Missing Powers to Compel Decryption in Bill C-59, Ticking Bombs, and the Future of the Encryption Debate* 57 ALTA L. REV. 267 (2019).
[634] Lee, *supra* note 609, at 126.
[635] Criminal Code, R.S.C, (1985) c. C-46, §185.
[636] R v. Araujo, (2000) 2 SCR 992, at ¶ 59.

organisations.[637] This exception was a result of "moral panic" in the wake of gang wars and terrorist activities and was a conscious attempt by the legislature to placate the citizens and assure them of their safety.[638] However, the scope of criminal organisations and terrorist activities have been vastly expanded by the legislature which practically allows the police to circumvent the investigative necessity requirement irrespective of such target being "associated" with such offences or not.[639]

Unlike the USA where there are clear provisions applicable to different types of services, Canada does not have such distinction. It is still ambiguous as to what provisions would apply for procuring text messages or email communications. An OCS provider such as WhatsApp, essentially acts as an intermediary who periodically produces text messages to two consumers and such type of service is a continuing service. If an officer needs access to the messages between two consumers, a general search warrant or an assistance order, cannot be squarely applicable to such service simply because the service provider performs the dual role of storing and also providing messaging services at all times. In this context, the Canadian SC[640] categorised such search and seizure as interception and ruled that it requires an assistance order and not a general search warrant The Canadian SC was however split as to its reasons, with three of the justices relying on

---

[637] Criminal Code, R.S.C, (1985) c. C-46, §186.
[638] Jim Cruess, *Cost of Admission: One Rubber Stamp-Evaluating the Significance of Investigative Necessity in Wiretap Authorisations after R v. Araujo*, 32 DAL J OF L STUDIES 55, 65 (2013).
[639] *Id.* at 66.
[640] R v. TELUS Communications & Co., 2013 SCC 16.

the fact that data was procured "during transmission", while the other two justices relied on the nature of warrant sought which in this case was "prospective".[641]

iii. Encryption and Assistance Order

Although an Assistance Order can mandate a third party/any person to provide technical assistance to the law enforcement, it is unclear as to whether it could be used to mandate decryption.[642] There has also not been an instance before the court where it was required to mandate a third party to break an encryption to assist the court's investigation. The Assistance Order, however, could be issued by the judge to compel the owner of the personal device to decrypt the phone. The Canadian SC, after asserting that such compulsion is nothing short of compelled speech, held that encryption and the laws against self-incrimination could not be used to completely prevent the access of law enforcement to material evidence.[643] Subsequent to an emphasis on this caveat, the Canadian SC after assessing the facts of the case, came to a different conclusion in the end by holding that in balancing the competing interests of the State's access to evidence and the target's right to remain silent, the latter survived.[644] Unlike USA, the courts in Canada have emphasised on deciding upon the question of self-incrimination and privacy on a case to case basis.

---

[641] Susan*, supra* note 616, 512.
[642] Steven Penney & Dylan Gibbs, *Law Enforcement Access to Encrypted Data: Legislative Responses and the Charter,* 63 MCGILL L J 201, 211 (2017).
[643] R v. Shergill, (2019) ONJC 54, ¶ 46.
[644] *Id.* at ¶ 132.

C. UNITED KINGDOM

The UK does not have a written constitution but has incorporated the rights in the European Convention on Human Rights [*hereinafter* "**ECHR**"].[645] Article 8 of the ECHR[646] protects the right to privacy of the citizens.[647] The threshold, however, for a state to reasonably intrude into one's privacy is determined by the legality, necessity and proportionality of the intrusion.[648] In assessing proportionality, it looks at whether relevant and sufficient reasons are advanced by the state concerned for justifying an intrusion.[649]A supplementary requirement that the ECHR requires for the intrusion to be reasonable is that it must be "reasonably foreseeable", *i.e.*, the citizens must be made aware in uncertain terms the instances in which the State would intrude into one's privacy.[650]

The framework of UK is recapitulated in Investigatory Powers Act, 2016. This Act was preceded by the Regulation of Investigative Powers Act, 2000 which was subject to severe criticism because it lacked provisions mandating judicial pre-authorisation of digital searches.[651]

---

[645] Human Rights Act, 1998 (Eng.).
[646] Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5, Art.8.
[647] Joyce W Luk, *Identifying Terrorists: Privacy Rights in the United States and the United Kingdom*, 25 HASTINGS INT'L & COMP L REV 223, 248 (2002).
[648] Handyside v. The United Kingdom, [1976] ECHR 5, ¶49.
[649] *Id.*
[650] Big Brother Watch v. U.K., [2018] ECHR 722.
[651] *Id.* at 254.

i. Warrant Requirement for Content Information

The law does not contemplate any consent requirement from the subject of the investigation. ECHR jurisprudence broadly classifies search and seizure as 'covert' or 'coercive' surveillance.[652] In terms of covert surveillance the type of data to be accessed is classified and the law clearly distinguish between "content of communications"[653] and "communications data",[654] which corresponds to content and non-content information respectively. However, the text does not in any manner suggest a threshold except for such search to be necessary and proportional. Much of the burden of developing the proportionality test was left to the judiciary, which anyway is subjected to the principles propounded by the ECHR on the vires of proportionality test several times.[655]

Any warrant irrespective of the type of data sought to be procured needs to be authorised by the Judicial Commissioner before the same is authorised by the Secretary of State.[656] Even though there is an urgency exemption, the warrant must be approved by the Judicial Commissioner within three days of its issue failing which it ceases to be operative.[657]

---

[652] *See generally,* Bernard Keenan, *State Access to encrypted data in the U.K: The "Transparent" Approach*, COMM. L W REV. (2019), https://eprints.bbk.ac.uk/id/eprint/29734/, (last visited September 29, 2020) ("**Bernard Keenan**").
[653] Investigatory Powers Act 2016, cl. 261(6).
[654] *Id.* cl. 261(5).
[655] *See* The Sunday Times v. United Kingdom, Eur. Ct. H. R. 49 (1979); Handyside v. The United Kingdom, Eur. Ct. H. R. 48 (1976).
[656] Investigatory Powers Act 2016, cl. 23.
[657] *Id.* at cl. 24.

ii. Encryption

Encryption engages the provisions regarding 'coercive' surveillance where the third party or the accused himself is coerced into decrypting the data obtained lawfully by the law enforcement.[658] The disclosure notice[659] in the Regulation of Investigative Powers Act mandates that the law enforcement could mandate either the third party or the target of the investigation to decrypt the data. The provision is applicable to a broad range of data defined as 'protected data' and to person who is in possession or control of the decryption key. The prosecution has the burden to prove that the key is in possession and control of the intended recipient of the notice; the recipient also has an opportunity to deny the same with adequate proof.[660]

Another mode of 'coercive' surveillance is by issuing the Technical Compatibility Notice [*hereinafter* "**TCN**"]. A TCN requires the service provider to grant technical assistance in any manner with the sole objective of ensuring that the intermediary has the ability to assist a lawful interception as long as it is reasonable and practicable to do so.[661] A TCN could be issued by the Secretary of the State only if it is authorised by a Judicial Commissioner.[662] The scope of TCN has been amplified under IPA

---

[658] Bernard Keenan, *supra* note 652, 20.
[659] Regulation of Investigatory Powers Act, 2000, § 49.
[660] STEPHEN MASON, ELECTRONIC SIGNATURES IN LAW (Cambridge University Press, 2012).
[661] Investigatory Powers Act 2016, cl.253.
[662] *Id.* at cl. 254.

and could be issued at any time irrespective of such notices complementing a disclosure notice or not.[663]

The England and Wales Court of Appeals held that compelling a person to produce the decryption key is similar to a key for a brief case or a purse, and the material inside the device would be intelligible and *"only be revealed for what it is"* as the key exists independent of the evidence (the contents of the briefcase/electronic device) itself.[664] The courts still emphasise on the need to prove that the person is in possession of the key.[665] The concept of self-incrimination is discussed in detail in the context of child pornography and terrorist acts, with the verdicts thus far being more or less in favour of the State.[666]

iii. Synthesising Lessons from other Jurisdictions

In comparing all these aforementioned foreign jurisdictions, we can clearly observe the different approaches these countries take in ensuring protection to privacy. Arguably these jurisdictions also fall short of an ideal framework. While USA and Canada have refrained from conclusively deciding on the question of encryption, the all-encompassing proportionality test in UK has subsumed and also theoretically justified, coercing subjects and third parties to provide passwords and decryption keys. However, USA's framework, even though fragmented, seems more

---

663 Bernard Keenan, *supra* note 652*,* 11.
664 R v. S, [2008] EWCA Crim 2177, ¶ 18.
665 *Id; see also* Greater Manchester Police v. Andrews, [2011] EWHC 1966 (Admin), ¶¶ 20-22.
666 Bela Chatterjee, *Fighting Child Pornography through UK Encryption Law: A Powerful Weapon in the Law's Armoury,* 24 CHILD & FAM L Q 410, 418 (2012).

sophisticated and tailored in addressing privacy concerns in digital searches, and above all there is correlation between the judge made law and legislations. On the contrary, Canada's framework presents a dichotomy of approach by the legislature and the judiciary, essentially cancelling out each other's effect rendering the law majorly ambiguous.

These differences could be attributable to the underlying differences in their search and seizure jurisprudence. It could also be attributable to the reluctance of topmost courts in Canada to specify tests and principles, which is also understandable given the dynamic nature of technology itself. As for digital searches, unlike India there are tailored procedures for each type of data or digital search/surveillance in all these countries. Lastly, none of these countries lack pre-judicial authorisation.

V. SUGGESTIONS: THE WAY FORWARD

A. ACKNOWLEDGING THE METAPHOR PROBLEM AND TAILORING PROCEDURAL SAFEGUARDS

As it could be inferred from the discussion above, the attempts by courts in USA, UK and Canada in addressing the metaphor problem could be attributable to the explicit provisions their constitutions regarding the negative obligation of the state in search and seizure. In the course of developing such privacy jurisprudence, a conscious attempt at understanding the implications on the right to privacy of a person in case of digital searches and distinguishing them from traditional searches seems to have been the first step in other jurisdictions.

The subsequent step would be to relinquish traditional rules and procedures followed in search and seizure and formulate new ones more appropriate for digital evidence. It is also argued that even specification of folders or locations within the cyber space in the warrant would be necessary to ensure that the digital search is "reasonable".[667] Minimization requirements within warrants were not considered a constitutional mandate, despite knowing that a digital search is more invasive because of the inherent contingency and unpredictability that a digital search and seizure entails.[668] However, the logic of the metaphor problem has managed to trickle down, and lower courts in the USA seem to be exercising the power to prescribe protocols and minimisation requirements as and when necessary.

Moreover, the impact of having recognized privacy as a fundamental right, on the search and seizure powers of the State has to be necessarily revisited. The procedure of search and seizure in India has not deviated much from the archaic pre-colonial principles and is significantly influenced by decisions of the Supreme Court immediately after independence.[669] Even in cases of interception, the courts and the law prevalent is significantly influenced and constrained by the guidelines formulated in *PUCL*. The very conflict between privacy and law

---

667 Michael Mestitz, *Unpacking Digital Containers: Extending Riley's Reasoning to Digital Files and Subfolders,* 69 STAN L REV 321 (2017).
668 Kerr, *supra* note 564, 575.
669 *Kathi Kalu*, *supra* note 532; *M. P. Sharma*, *supra* note 516.

enforcement needs to be considered in light of the new *Privacy Judgement* and the techno-legal crisis that digital evidence presents.

B. ROLE OF THIRD-PARTY AND THE CONSENT REQUIREMENT

The case of *District Registrar & Collector v. Canara Bank*[670] has rejected the application of the third-party doctrine by expressly rejecting the *US v. Miller* case;[671] this was further affirmed by the *Privacy Judgement*.[672] However, in India the law enforcement has unconstrained access to data of citizens available with third parties. The provisions authorising such production are buried in the due diligence guidelines. This it is not only highly unsettling, but there arises a very important question as to whether such authorisation by the guidelines of the executive could be considered 'law' for the purpose of the proportionality test. In India, the legislature cannot delegate its essential functions, involving acts of laying down policy of the law and enacting that policy into a binding rule of conduct.[673] Considering the judgements by the Supreme Court on excessive delegations, it could be argued that entirely shifting the responsibility of protecting fundamental rights to the executive without any legislative guidance[674] is arbitrary and an excessive delegation of legislative powers and is thus, violative of Article 14 of the Constitution[675] as well.

---

[670] District Registrar & Collector v. Canara Bank, (2005) 1 SCC 496.
[671] Gautam Bhatia, *State Surveillance and the Right to Privacy in India: A Constitutional Biography,* 26 NAT'L L SCH INDIA REV 127, 151-152 (2014).
[672] *Privacy Judgement*, *supra* note 475, ¶ 77.
[673] In re The Delhi Laws Act, 1912, AIR 1951 SC 332; Hamdard Dwakhana v. Union of India, 1965 AIR SC 1167; M.L. Jain v. India AIR 1989 SC 669.
[674] Interception Rules, *supra* note 549, r. 4, 5, 8 & 22.
[675] INDIA CONST., Art.14.

The Supreme Court for the first time, albeit narrowly, had conceptualised privacy in terms of individual autonomy and liberty, and thereby striking down overbroad provisions in the U.P. Police Regulations that allowed for complete discretion to the police to enter any premises.[676] This moral argument for personal autonomy is crucial because later, in cases of balancing between right to free speech and right to privacy (private life), the Supreme Court[677] has held that even if a person's personal information is available to the public by way of their fame/position in society, materialisation of the same in any medium and the manner of the same could be justified only if the concerned person has given their consent. That is to say that the autonomous right to divulge one's personal information and the liberty to do so being guaranteed under Article 21, explicit consent plays an important role in justifying an encroachment, irrespective of such information being divulged voluntarily to any third party or the general public. Unfortunately, this consent requirement has not been inculcated in the search and seizure regime in India, due to the adherence to the Crime Control Model.

The Supreme Court in the case currently under consideration would hopefully decide on the broader question of the extent of assistance that the third party could be providing, procedural requirements and under what circumstances consent of the customer is necessary for a digital search to pass the test of proportionality as propounded in the *Privacy Judgement*.

---

[676] Gobind v. State of Uttar Pradesh, 1975 2 SCC 148, ¶ 24, 28.
[677] R. Rajagopal v. State of T.N., (1994) 6 SCC 632.

Given that consent by a subscriber of a particular service in respect of their personal information provided to the intermediary could never be equated to an informed consent,[678] using such consent to conclude that the citizen does not have reasonable expectation of privacy, as seen in Canada, is problematic. The courts in India must also take into consideration that such consent could not said to be given out of exercising their free will when it is "unwitting, coerced or incapacitated"[679] by extraneous pressures involved in making that decision. Which is why the consent requirement as stipulated in the USA could be a better choice in legitimising the procurement of digital evidence, *i.e.*, requiring consent before a seizure takes place, instead of transposing the consent given to intermediary as one that is indirectly given to the State.

C. ENCRYPTION- ANONYMITY UNDER ARTICLE 21

The judiciary would have to primarily decide on the extent of protection that Article 21 provides for anonymity. The 9-judge bench in the *Privacy Judgement* has clearly distinguished anonymity and privacy, but in terms of anonymized metadata and a legitimate state interest of procurement and perusal of the same (context of metadata and mass surveillance).[680] However, the ambit of Article 21 with respect to an

---

[678] Nupur Chowdhury, *Privacy and Citizenship in India: Exploring Constitutional Morality and Data Privacy*, 11 NUJS L REV 421, 426, 427 (2018); *see also, Justice Sri Krishna Committee Report, Free and Fair Digital Economy* (2019), 32-37, https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf (last visited September 9, 2020).

[679] Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent,* 96 WASH U L REV 1461, 1466 (2019).

[680] *Privacy Judgement*, *supra* note 475*,* ¶ 312.

individual and his expectation of anonymity in cyberspace has not been considered and delved into in the *Privacy Judgement* or thereafter. Canada has specifically entertained the notion that encryption shall not determine the existence of a reasonable expectation of privacy and that a requirement to decrypt would have to be determined on a case-to-case basis.[681] The judiciary in accommodating encryption and its privacy implications is also provided with the crucial task of choosing an appropriate metaphor.

In case of compelling the accused to produce the key, it depends on how the court interprets the act of providing the key by the accused.[682] The emphasis on what is being produced and equating it to a key for a safe box is problematic, as it disregards the role of the accused in rendering that information accessible and intelligible.[683] The courts in other jurisdictions discussed above have construed this conundrum in a manner where even when such compulsion would trigger the right against self-incrimination, it would still be construed as legitimate and reasonable compulsion.

The Supreme Court in *Kathi Kalu* has justified compulsion on the basis that such compulsion will not change the intrinsic character of the evidence. Applying the same logic, the content of the evidence already in existence and in possession of the police will not be altered in any manner by compelling the accused to produce the password. However, the role of the accused in incriminating himself and moreover in providing evidence

---

[681] Susan*, supra* note 616.
[682] *See generally,* Lex Gill, *supra* note 488.
[683] Bela Chatterjee, *Fighting Child Pornography through UK Encryption Law: A Powerful Weapon in the Law's Armoury,* 24 CHILD & FAM L Q 410, 419 (2012).

against himself under compulsion is completely disregarded, unlike the act-of-production doctrine followed in the USA. Moreover, the restriction of the scope of Article 22 to only testimonial evidence, could be revisited in light of the emergence of digital evidence.

D. JUDICIAL PRE-AUTHORISATION

The framework for judicial pre-authorization in USA is influenced by historical factors, refraining from adopting colonial laws and a heightened emphasis on citizen's privacy.[684] Granting such excessive powers to the executive is much less preferable when compared to the constitutional scrutiny of a neutral body like the judiciary.[685] Even in the UK the Investigatory Powers Act has adopted the system of prior judicial authorisation for the purpose of digital searches. However, in India, even though the law enforcement does have a 'legitimate state interest for the law to be reasonable; a neutral body by a mandatory *ex ante* warrant requirement overseeing digital searches is essential. Under no stretch of imagination could it be claimed that a procedure involving only the executive wing of the government to oversee and provide authorisations for law enforcement to infringe a citizen's fundamental right is a reasonable procedural safeguard.

---

[684] David G Barnum, *Judicial Oversight of Interception of Communications in the United Kingdom: An Historical and Comparative Analysis*, 44 GA J INT'L & COMP L 237, 292 (2016).
[685] *Id.* at 297.

E. LEGISLATIVE CLASSIFICATION OF TYPES OF DATA AND CLARITY IN LAW

The need for clarity in legislation which propounds to infringe upon one's privacy is mainly in adherence to the foreseeability principle, and the same has also been inculcated in India by the *Privacy Judgement*.[686] The Indian framework unlike the other jurisdictions does not acknowledge the different types of data that could help an investigation. Such classification is necessary for targeted procedural safeguards. It is desirable for such clarity to be present in the law, so that the citizens are aware of their rights and the procedures to be followed in a digital search. If the law framed is sufficiently precise to enable foreseeability, the judiciary would not be burdened in developing the law on case-by-case basis which is not only slower but could result in a lot of ambiguity and inconsistencies in the law.[687]

VI. CONCLUSION

The metaphor problem does not have a ready answer. It would even be a stretch to argue that the courts across the world have even understood the full extent and scope of the problem, or have successfully pre-empted the future problems that technological development could pose for digital searches and seizures. While the information that a person expects to keep private remains more or less the same throughout history, the vulnerability

---

[686] *Privacy Judgement*, *supra* note 475*,* 640.
[687] Timothy Azarchs, *Informational Privacy: Lessons from across the Atlantic,* 16 U PA J CONST L 805, 822 (2014).

and susceptibility of such information is robustly changing in the digital sphere. This paper has attempted to demonstrate the uncertainty and obscurity of the metaphor problem itself, which is captured by the subjective nature of the proportionality test used by UK, and the case-by-case approach adopted by the Canadian courts. While it is difficult to characterize the regime in USA, its attempt to objectively determine privacy right isn't entirely ideal.

This paper has also made efforts to explain in detail the great emphasis these legal systems place on procedural safeguards. It emanates from the fact that these legal systems have a constitutional mandate for reasonable search and seizure. On the contrary, in India due to the lack of any definitive notion of privacy, the law governing searches and seizures has evolved into a very oppressive regime, in juxtaposition to the other precocious legal systems discussed above. The author, analysing the legal system in India highlighted that the Supreme Court in the *Privacy Judgement*, does little to overcome *M. P. Sharma* and *Kathi Kalu,* which has assertively reinforced colonial notions of crime control post-independence. Problems such as lack of clarity in laws governing search and seizure, excessive delegation of powers to executive to adjudicate on matters of fundamental rights, inadequate if not absolute lack of procedural safeguards in respect of digital searches denotes excessive crime control. This is further aggravated by the fact that both the legislature and the judiciary in India is blind to the metaphor problem. Unless our legal system reforms radically to take account of these issues, it will render the right to privacy superficial.