SELF-INCRIMINATION AND DIGITAL EVIDENCE: PROPOSING A FRAMEWORK POST VIRENDRA KHANNA

Vadita Agarwal & Tanishq Kabra[*]

The Karnataka High Court in its Virendra Khanna *v.* State of Karnataka *('Virendra Khanna') judgment pronounced that compelled decryption of electronic devices by the accused in a criminal case was not violative of the right against self-incrimination or the right to privacy. Though Virendra Khanna was subsequently held to be per incuriam in* CBI *v.* Mahesh Kumar Sharma*, India's position on the intersection between self-incrimination and digital evidence is nascent at best. After analysing the incompatibility of Virendra Khanna with India's established principles of self-incrimination, the paper argues for an adoption of principles of the Foregone Conclusion Doctrine from the United States. This adoption is demonstrated as viable in light of first, the similarity between Indian and American law on the subject of the right against self-incrimination and second, the petition submitted before the Supreme Court to lay down guidelines for seizure of electronic devices. The paper also argues for harmonising the law when it comes to different forms of decryption such as passwords or biometrics. An implication of the argument adopted by the paper is creating a new zone of privacy for cell phones, given their dynamic and intrusive nature. Ultimately, the paper pre-empts a rebuttal to its argument in the form of the Third-Party Doctrine and refutes that.*

TABLE OF CONTENTS

[*] 4th and 3rd year B.A. LL.B (Hons.) students at the West Bengal National University of Juridical Sciences, Kolkata.
The authors would like to thank the NUJS Law Review for their comments. All errors, if any, are solely attributable to the authors.
The authors may be reached at vadita221052@nujs.edu and tanishq222117@nujs.edu for feedback or comments.

I. INTRODUCTION

In a writ petition before the Karnataka High Court ('Karnataka HC'), in the case of *Virendra Khanna* v. *State of Karnataka* ('Virendra Khanna'), in answering whether an accused can be compelled to unlock his electronic device to obtain evidence, the Court answered in the affirmative and held that the compelled disclosure of a password does not violate the right of the accused against self-incrimination.[1] Primary among the reasons elucidated by the Court for this holding was that the rules which apply to physical documents with private information cannot be transposed to smart phones or other electronic equipment with equivalent information.[2] Only a few months later, in *CBI* v. *Mahesh Kumar Sharma* ('Mahesh Kumar Sharma'), a Delhi Sessions Court declared Virendra Khanna to be *per incuriam*.[3] While a formal overruling of Virendra Khanna by the Supreme Court ('SC') would be ideal, the principles laid down in Mahesh Kumar Sharma are nonetheless worth discussion. This is possibly the first time India has ventured into the interplay between digital evidence and the constitutional right against self-incrimination.[4]

With private conversations increasingly moving online, there need to be measures in place to limit state surveillance over the activities that individuals undertake in the digital realm. Attempts to subvert digital privacy are apparent, for instance, in the rules of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ('IT Rules'), directing social media intermediaries to identify originators of a message in case of an order by a competent authority.[5] With the IT Rules still receiving pushback from significant social media intermediaries such as WhatsApp,[6] the debate surrounding self-incrimination *vis-a-vis* digital relevance becomes increasingly relevant. By giving investigating officials, and by extension, the State, unfettered access to digital devices, judgments such as Virendra Khanna take the cell phone out of the possession of the owner and render important ongoing debates about privacy in India moot.

Article 20(3) of the Indian Constitution provides a constitutional guarantee to the accused against self-incrimination.[7] To decide whether the right against self-incrimination is violated, three questions need to be answered affirmatively. First, if the person is accused of an offence; second, if the person is required to give evidence against himself; and third, if the

[1] Virendra Khanna v. State of Karnataka, 2021 SCC Online Kar 5032 ('Virendra Khanna').
[2] *Id*., ¶15.3.
[3] CBI v. Mahesh Kumar Sharma, 2022 SCC OnLine Dis Crt (Del) 48 ('Mahesh Kumar Sharma').
[4] The Constitution of India, 1950, Art. 20(3).
[5] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, R. 4(2); *See* Krishnesh Bapat et al, *Deep Dive: How the Intermediaries Rules are Anti-Democratic and Unconstitutional*, INTERNET FREEDOM FOUNDATION, February 27, 2021, available at https://internetfreedom.in/intermediaries-rules-2021/ (Last visited on August 8, 2024).
[6] *See* NDTV, *"If We're Told to Break Encryption, WhatsApp Goes": Platform's Big Warning*, April 26, 2024, available at https://www.ndtv.com/india-news/whatsapp-delhi-high-court-if-were-told-to-break-encryption-whatsapp-goes-platforms-big-warning-5526190 (Last visited on July 8, 2024).
[7] The Constitution of India, 1950, Art. 20(3).

person is 'compelled' to incriminate himself.[8] As explained in *State of Bombay* v. *Kathi Kalu Oghad* ('Kathi Kalu Oghad'), while every positive volitional act which produces evidence is a testimony, testimonial compulsion, which Article 20(3) provides a guarantee against connotes coercion "which procures the positive volitional evidentiary acts of the person, as opposed to the negative attitude of silence or submission on his part".[9]

While the Karnataka HC was the first to address the question of digital evidence in the context of self-incrimination, its findings rationalised into a larger scheme of what journalists and commentators describe as a backsliding of data privacy in India.[10] As per data released by the National Crime Records Bureau in its 2022 report, India has witnessed a consistent rise in cybercrimes over the years, particularly those targeted towards women and Scheduled Castes.[11] Furthermore, with a rising trend of the state encouraging seizure of electronic devices of journalists and other dissenters,[12] creating appropriate safeguards for the protection of their constitutional right against self-incrimination becomes increasingly important. In this context, the paper critiques Virendra Khanna and provides alternate solutions using a contemporary understanding of self-incrimination and privacy in digital devices. While Mahesh Kumar Sharma does, to a large extent, mitigate the shortcomings of Virendra Khanna, it fails to lay down a positive framework on the law on compelled decryption in India. While Mahesh Kumar Sharma's guidelines are largely prohibitory in nature, the paper aims to lay down the limited framework in which decryption can be compelled without the risk of self-incrimination by the accused and create clearly defined boundaries around the act. The paper heavily makes use of United States of America ('U.S.') jurisprudence since their understanding of this subject is arguably the most nuanced. The Foregone Conclusion Doctrine arises in the context of the Fifth Amendment to the U.S. Constitution, which protects individuals from being compelled to incriminate themselves.[13] The Foregone Conclusion Doctrine states that when a suspect's act of production of documents contains evidence which does not communicate any information which the government was not already aware of, then that act of production is a "foregone conclusion" and the Fifth Amendment privilege does not apply.[14]

Part II analyses the primary findings of Virendra Khanna, showing how at its very core, it errs in its understanding of self-incrimination. It then discusses the limited, contrary ruling in Mahesh Kumar Sharma. Part III of the paper briefly justifies the reliance on the U.S. Foregone Conclusion Doctrine by demonstrating the similarity between the U.S. and Indian law on self-incrimination. Part IV of the paper is dedicated to understanding the

---

[8] Abhinav Sekhri, *The Gujarat High Court's Voice Spectrograph Decision- II: Guest Post- Between a Rock and a Hard,* CONSTITUTIONAL LAW AND PHILOSOPHY, February 17, 2017, available at https://indconlawphil.wordpress.com/tag/article-203/ (Last visited on July 10, 2023).

[9] State of Bombay v. Kathi Kalu Oghad, (1962) 3 SCR 10, ¶8 ('Kathi Kalu Oghad').

[10] Justin Sherman, *India's Sudden Reversal on Privacy Will Affect the Global Internet*, THE WIRE, September 10, 2022, available at https://thewire.in/rights/india-privacy-data-protection-global-internet-effect (Last visited on July 8, 2024); Panthea Pourmalek & Danielle Luo, *In India, Data Protection Is Expanding State Power*, CENTRE FOR INTERNATIONAL GOVERNANCE INNOVATION, October 2, 2023, available at https://www.cigionline.org/articles/in-india-data-protection-is-expanding-state-power/ (Last visited on July 8, 2024).

[11] Mahender Singh Manral & Jignasa Sinha, *24% rise in cybercrime in 2022, 11% surge in economic offences: NCRB report*, INDIAN EXPRESS, December 4, 2024, available at https://indianexpress.com/article/india/rise-cybercrime-2022-economic-offences-ncrb-report-9053882/ (Last visited on July 8, 2024).

[12] Tanishka Sodhi, *'Incomplete Reports', 'Financial Toll'- The Burden of Digital Device Seizures on Journalists, Outlets*, NEWSLAUNDRY, NOVEMBER 8, 2023, available at https://www.newslaundry.com/2023/11/08/incomplete-reports-financial-toll-the-burden-of-digital-device-seizures-on-journalists-outlets (Last visited on July 8, 2024).

[13] The Constitution of the United States of America, 1789, Amendment V.

[14] Doe v. United States (*In re* Grand Jury Subpoena), 383 F.3d 905, 910 (9th Cir. 2004) (United States Court of Appeals for the Ninth Circuit).

Foregone Conclusion Doctrine as seen in U.S. jurisprudence and the scholarly debate on the same. Highlighting the two camps that case laws and scholars of this Doctrine usually fall into, the paper corroborates one view based on an understanding of the right against self-incrimination and cell phone privacy. Part V discusses the applicability of the Foregone Conclusion Doctrine in India and its concomitant challenges. Part VI of the paper lays down the legal justification for a necessary implication of the argument the paper adopts, that is, the creation of a new zone of privacy for cell phones. Part VII briefly discusses an anticipated objection to the argument of the paper in the form of the Third-Party Doctrine and rebuts it. Part VIII concludes the paper.

II. DECONSTRUCTING VIRENDRA KHANNA

The Karnataka HC in Virendra Khanna held that in a criminal case, compelled decryption of an electronic device and consequent accessing all the data on the device does not violate the accused's right against self-incrimination.[15] This part of the paper will first dissect the Virendra Khanna ruling to understand the rationale used by Karnataka HC in reaching its decision. As a preliminary inquiry, the incompatibility of the Virendra Khanna ruling with established principles of self-incrimination will be discussed. Ultimately, the contrary ruling by a Delhi District Court in Mahesh Kumar Sharma and its reasoning in declaring Virendra Khanna to be *per incuriam* will be discussed.

A. ANALYSING THE PRIMARY FINDINGS

While understanding this case, it is necessary to question the certain legal frameworks, which have been interpreted in Virendra Khanna to permit law enforcement agencies to request access to a digital device in order to further their investigation and what legal restrictions, if any, apply to law enforcement when they "explore" a digital device's contents for investigative purposes.

As correctly identified in Virendra Khanna, the Code of Criminal Procedure, 1973 ('CrPC'), provides a framework for the search of physical premises and does not specifically address the question of seizure of electronic evidence.[16] The provisions governing search and seizure in the CrPC in the ordinary course of investigation detail the requirement of a search warrant which can be issued under §93 of the CrPC.[17] In emergency circumstances, if the officer in charge of a police station reasonably believes that anything necessary for the purposes of an investigation into an offence which he is authorised to investigate cannot be "obtained without undue delay", he may undertake search without a warrant as well.[18] In either case, the obligation imposed upon the accused under §100 of the CrPC is to allow the officer free ingress into the place against which the warrant has been executed if the place is locked.[19]

In the context of digital evidence, Virendra Khanna interpreted §100 of the CrPC to mean that the accused would have to provide the investigating officer access to a seized electronic device by providing its passcode or biometric password to unlock the

[15] Virendra Khanna, *supra* note 1, ¶5.9.
[16] *Id*., ¶12.3.
[17] The Code of Criminal Procedure, 1973, §93.
[18] *Id*., §165.
[19] *Id*., §100.

device.[20] It was this act of decrypting the device which was held in Virendra Khanna to not amount to self-incrimination.[21]

Before making a determination on the issues of the case, the HC contextualised the ubiquity of electronic evidence as one which has rendered "anything on paper…obsolete".[22] Given that traditionally, physical evidence has taken an electronic appearance, the HC noted that access to evidence which is essential to a criminal investigation is not possible without decrypting the device in question.[23] In light of this, the HC held that in the course of a criminal investigation, the Investigating Officer can direct the accused to furnish information to assist the investigation, and further, he can also direct the accused to provide the password to his electronic device.[24]

The HC permitted compelled decryption of the device under §102 of the CrPC in emergent circumstances, such as "if the data is going to be immediately destroyed, there is a danger of equipment itself being destroyed, the possibility of the equipment not being available, etc".[25] In analysing this provision of the CrPC, the HC admitted that the threshold to prove suspicion of commission of an offence which can make the Investigating Officer do away with the requirement for a warrant is "wide enough to cover a plethora of situation(s)".[26] With a general lack of jurisprudence and general guidelines for investigating officers on how to handle electronic evidence, individual privacy is essentially left to the subjective interpretation of the state.

Ultimately, the judgment provided two reasons for justifying why compelled decryption in this scenario would not amount to a testimonial compulsion. First, in drawing a parallel with Kathi Kalu Oghad, it held that since providing thumb impressions or writing specimens does not incriminate the accused, providing access to, say, a cell phone, would not incriminate the accused either.[27] Second, it held that in any case, any evidence obtained during the course of investigation would have to be proved in a court of law by using the "applicable rules of evidence". Thus, the principle used by the HC in holding compelled disclosure of password to not be self-incriminatory was that by doing so, the accused is not compelled to make any oral or written statement which could incriminate him.[28] As will be discussed in detail in the subsequent portion of the paper, Virendra Khanna reaches its conclusion by equating fingerprints, as discussed in Kathi Kalu Oghad, with biometric information used to unlock a cellphone, and isolating the latter from the resulting consequence of an unlocked electronic device. Briefly, the reason why Kathi Kalu Oghad held the production of fingerprints to not be self-incriminatory was that fingerprints, or even handwriting samples, "by itself" do not have a tendency to incriminate the accused.[29] They are largely unchangeable and only useful for comparisons "in order to lend assurance to the Court that its inference based on other pieces of evidence is reliable".[30]

The judgment goes as far as to say that in the event the accused refuses to cooperate with the investigating agency, they would be at liberty to clone the device or change

[20] Virendra Khanna, *supra* note 1, ¶9.1.
[21] *Id*., ¶¶14.1-14.8.
[22] *Id*., ¶8.13.
[23] *Id.*, ¶12.13.
[24] *Id*., ¶9.1.
[25] *Id*., ¶12.13.
[26] *Id*., ¶12.15.
[27] *Id*., ¶14.2.
[28] *Id*., ¶14.8.
[29] Kathi Kalu Oghad, *supra* note 9, ¶12.
[30] *Id*.

the passwords of the email so that no one but the designated officers would have access to the data of the accused.[31] The Karnataka HC also goes on to observe that the utilisation of aforementioned data during the course of inquiries would not constitute an infringement upon the right to privacy, as it was safeguarded within the delineated exceptions.[32]

Additionally, these findings are accompanied by an acknowledgement by the HC that once an investigating agency has access to an electronic device like a smart phone, it has "free access to all data not only on the said equipment but also any cloud service that may be connected to the said equipment, which could include personal details, financial transactions, privileged communications and the like".[33] Thus, not only does Virendra Khanna not impose any limits on the permitted access to cell phones, it acknowledges the level of intrusion such a limitless search could cause.

B. INCOMPATIBILITY WITH THE EXISTING JURISPRUDENCE ON SELF-INCRIMINATION

Before exploring the nuances of digital evidence, it is important to note that Virendra Khanna errs in identifying the fundamental principles of self-incrimination. It was infamously held in Kathi Kalu Oghad that compelling production of fingerprints does not incriminate the accused.[34] Drawing a parallel with Kathi Kalu Oghad, among a catena of unsubstantiated generalisations, Virendra Khanna held that providing access to an email or mobile phone would not amount to self-incrimination,[35] since the accused would be required to prove the document by other evidence as well.[36]

The direct correlation in Virendra Khanna between physical evidence, as envisaged in Kathi Kalu Oghad and biometric information or passwords is manifestly problematic. Kathi Kalu Oghad categorically held that only that evidence, which, if considered in isolation, has the ability to incriminate the accused, falls under the guarantee against testimonial compulsion.[37] This is in contrast to evidence such as fingerprints or signatures which are first, largely unchangeable; leaving no scope for the accused to tamper with them and second, only incriminate the accused when compared with other evidence on record.[38] The unchangeable nature of this evidence is significant since despite possible attempts by the accused to change the nature of the evidence, its intrinsic nature is unalterable.[39]

Since documentary evidence can also be self-incriminating in nature,[40] the simple logical link between unlocking one's phone and handing it over to an investigating agency leaves a host of data and information which could incriminate the accused at the behest of the investigating officer. An additional clarification raised in Kathi Kalu Oghad was that the accused person can incriminate himself not only by imparting his knowledge but also through the "production of documents which though not containing his own knowledge would have a

[31] Virendra Khanna, *supra* note 1, ¶16.7.
[32] *Id*., ¶15.5.
[33] *Id*., ¶15.2.
[34] Kathi Kalu Oghad, *supra* note 9, ¶11.
[35] Virendra Khanna *supra* note 1, ¶9.1.
[36] *Id*., ¶12.22.
[37] Kathi Kalu Oghad, *supra* note 9, ¶12.
[38] Gautam Bhatia, *Compelling an Accused to Unlock their Mobile Phones: A Critique of the Kerala and Karnataka High Court Judgements,* CONSTITUTIONAL LAW AND PHILOSOPHY, February 7, 2022, available at /https://indconlawphil.wordpress.com/2022/02/07/the-kerala-high-court-rules-on-mobile-phone-data-and-the-right-against-self-incrimination-a-critique/ (Last visited on July 10, 2023) ('Bhatia').
[39] Kathi Kalu Oghad, *supra* note 9, ¶11.
[40] *Id*., ¶11.

tendency to make probable the existence of a fact in issue or a relevant fact".[41] This is the standard which is currently adopted for considering evidence to be of an incriminatory nature. Applying the test in Kathi Kalu Oghad, an unencrypted device hosts a multitude of data which "makes the case against the accused person at least probable, considered by itself".[42]

What differentiates the evidence found on an unencrypted device from evidence which is not self-incriminatory such as fingerprints or blood samples is that the latter cannot, by themselves, incriminate the accused in the absence of comparison with other evidence, while the former can. On the point in Virendra Khanna that the evidence obtained would, in any case, have to be independently proven in a court of law, constitutional law scholar Gautam Bhatia correctly points out that the fact that a piece of evidence has to be proved in accordance with the applicable procedure is irrelevant to the question of self-incrimination.[43] As argued by Bhatia, if this consideration were relevant, paradoxically, even direct oral self-incriminatory statements would not warrant the protection of Article 20(3) since they too, have to be "proved and established" as per the Indian Evidence Act, 1872.[44]

Attempts to reconcile the rule against self-incrimination with the developing jurisprudence on digital evidence have been undertaken in other countries. Particularly, the paper focuses on the Foregone Conclusion Doctrine as propounded in the U.S. The subsequent portion of the paper will focus on a ruling contrary to Virendra Khanna by a Delhi Sessions Court.

C. SUBSEQUENT DEVELOPMENT: CBI v. MAHESH KUMAR SHARMA

The Delhi Sessions Court, in Mahesh Kumar Sharma, categorically held Virendra Khanna to be *per incuriam*.[45] It is pertinent to note that the Sessions Court, in this, case laid down different rules for unlocking a device using biometrics and passwords.[46] While this will be discussed at length in Part V, the general rule laid down was that, while compelling an accused to unlock his cell phone using a manually inserted password was an impermissible testimonial compulsion, compelling him to do so using biometric information was not.[47]

It was held in *Selvi* v. *State of Karnataka* ('Selvi') that "to be a witness", and thus to violate the guarantee against testimonial compulsion as used in Article 20(3), means "imparting knowledge in respect of relevant facts" 'via' oral or written statements, by a person who has personal knowledge of these facts.[48] Extensively citing Selvi, Mahesh Kumar Sharma held that when an accused discloses his password to the investigating agency,[49] he is required to apply his mental faculties and the same falls within the category of a "testimonial fact".[50] The mental faculties applied by the accused in reproducing a memorised password "purely based on his personal mental effort or knowledge" helped the Court distinguish these passwords from biometric information.[51] The rationale used by the Court was that while the password alone does not constitute a self-incriminating testimony, the goal of the password in

[41] *Id*., ¶27.
[42] *Id*., ¶12.
[43] Bhatia, *supra* note 38.
[44] *Id*.
[45] Mahesh Kumar Sharma, *supra* note 3, ¶36.
[46] *Id*., ¶27.
[47] *Id*., ¶¶27, 36.
[48] Selvi v. State of Karnataka, (2010) 7 SCC 263, ¶180 ('Selvi').
[49] Password in this case not referring to biometric passwords like fingerprints, but a passcode which is usually an alphanumeric combination which a person manually enters into the device.
[50] Mahesh Kumar Sharma, *supra* note 3, ¶36.
[51] *Id*.

the larger context of decryption is for the purpose of accessing the data stored in a device.[52] Compelled decryption of any sort was also held to expose the accused to disclosure of incriminating information, violating §161(2) of the CrPC, according to which the accused has a right to maintain silence regarding information which has a "tendency to expose him to a criminal charge".[53] As clarified by the SC in *Nandini Satpathy* v. *P.L. Dani* ('Nandini Satpathy'), §161(2) and Article 20(3) are "substantially the same".[54] In both provisions, the right to silence both during investigation and trial go beyond the case and protect the accused in regard to offences both pending and imminent by deterring him from disclosure of incriminatory matter.[55] Thus, effectively, the current position of law as per Mahesh Kumar Sharma is that compelling an accused to unlock his cell phone and hand it over to an investigating officer is a violation of, *inter alia*, the accused's right against self-incrimination.

Even though not in the nature of a conclusive overruling, which can be anticipated given repeated requests by the SC given its demand to the state to create guidelines for the seizure of electronic devices,[56] Mahesh Kumar Sharma goes a long way in curing the defects of Virendra Khanna. It does not, however, provide positive solutions on scenarios which the investigating agency can actually compel decryption. Having established the Indian position, the subsequent part of the paper will now analyse U.S. jurisprudence through the Foregone Conclusion Doctrine to create a holistic picture of access to digital evidence in the context of self-incrimination.

III. WHY THE UNITED STATES?

Before proceeding with the argumentation, it needs to be established why the paper argues that India should borrow from this particular foreign jurisdiction at all. Aside from the fact that Indian cases on privacy have routinely discussed and borrowed from U.S. jurisprudence,[57] this part briefly explores American law on searches in context of Indian law, justifying why an inter-jurisdictional analysis is both viable and beneficial in this regard.

The Fifth Amendment to the U.S. Constitution protects an individual from "being compelled in any criminal case to be a witness against himself".[58] Couched in similar terms is Article 20(3) of the Indian Constitution, which states that "no person accused of any offence shall be compelled to be a witness against himself".[59] This leads to two primary questions which form the foundation of understanding the right against self-incrimination in both jurisdictions. First, who does the privilege against self-incrimination extend to, and second, what makes a testimony self-incriminatory?

Regarding the first question on who can invoke the protection of Article 20(3), the initial position as laid down in Kathi Kalu Oghad was that 'at the time of making the statement', the person must have been the accused. Thus, it is not sufficient, for the purposes of Article 20(3) for the person to subsequently be exposed to a criminal charge.[60]

---

[52] *Id*., ¶37.
[53] The Code of Criminal Procedure, 1973, §161(2).
[54] Nandini Satpathy v. P.L. Dani, (1978) 2 SCC 424, ¶21 ('Nandini Satpathy').
[55] *Id*., ¶56.
[56] Awstika Das, S*eizure Of Journalists' Digital Devices A Serious Matter, Better Guidelines Needed To Protect Media Professionals : Supreme Court To Centre*, LIVE LAW, November 7, 2023, available at https://www.livelaw.in/top-stories/supreme-court-guidelines-search-seizure-digital-devices-241799?infinitescroll=1 (Last visited on July 8, 2024).
[57] *See* District Registrar and Collector, Hyderabad v. Canara Bank (2005) 1 SCC 496, ¶25 ('Canara Bank').
[58] The Constitution of the United States of America, 1789, Amendment V.
[59] The Constitution of India, 1950, Art. 20(3).
[60] Kathi Kalu Oghad, *supra* note 9, ¶16.

Acknowledging the position laid down in Kathi Kalu Oghad, Selvi laid down that while under Article 20(3) there exists the requirement of a formal accusation, §161(2) of the CrPC arguably lays down a wider protective net by covering "any person supposed to be acquainted with the facts and circumstances of the case".[61] Thus, as was upheld in Nandini Satpathy, the protection under §61(2) of the CrPC which "approximates the constitutional clause" of Article 20(3) shields those who have been formally exposed to a criminal charge; those who are examined as suspects in a criminal case as well as witnesses who have a reasonable apprehension that their answers could incriminate them.[62]

In fact, in Nandini Satpathy, Justice Krishna Iyer heavily borrowed from the dictum of *Miranda* v. *Arizona*, which laid down that statements stemming from custodial interrogation cannot be used as evidence unless the police officers have informed the accused of his right to remain silent,[63] to lay down that the right under Article 20(3) extends to investigation under the police level as well.[64] In U.S. jurisprudence as well, as held in *Hoffman* v. *United States*, the privilege against self-incrimination extends to witnesses in those situations where the witness "has reasonable cause to apprehend danger from a direct answer".[65] The rationale used by U.S. courts in allowing witnesses to invoke the privilege is the "cruel trilemma", that is, it being violative of human dignity to force a witness to choose among self-incrimination, perjury and contempt of the court.[66] Thus, witnesses must be given a fourth option of remaining silent without incurring criminal liability.

On the second question of what makes a testimony self-incriminatory, the Indian position answers the same, stating that a "reasonable tendency strongly to point out to the guilt of the accused are incriminatory".[67] As per Selvi, even information which leads to "derivative use", i.e., which leads to subsequent discovery of independent material and "transactional use", i.e., when information is helpful for investigation for offences other than the one being investigated can prove to be incriminatory.[68] The same principle applies to the U.S. as well. For the Fifth Amendment protection to apply, an act needs to be first, compelled, second, incriminating, and third, testimonial.[69] The implication is that the government can nonetheless compel a testimonial act as long as the one making it does not incriminate himself. In the case of *Hoffman* v. *United* States which has been routinely cited in Indian precedent,[70] the privilege extends not only to those answers which support a conviction under a criminal statute but those which "furnish a link in the chain of evidence needed to prosecute the claimant for a federal crime".[71] On what amounts to a testimonial act, verbal communication such as statements made in police custody or during a trial are almost always held to be testimonial in the U.S.[72] This is

[61] Selvi, *supra* note 48, ¶121.
[62] Nandini Satpathy, *supra* note 54, ¶21.
[63] Miranda v. Arizona, (1966) 384 US 436 (Supreme Court of the United States).
[64] Nandini Satpathy, *supra* note 54, ¶21.
[65] Hoffman v. United States, 341 U.S. 479, 486 (1951), 486-487 (Supreme Court of the United States) ('Hoffman').
[66] Murphy v. Waterfront Commission of New York, 378 U.S. 52, 55 (1964) (Supreme Court of United States); Twining v. New Jersey, 211 U.S. 78, 91 (1908) (Supreme Court of the United States); Ullmann v. United States, 350 U.S. 422, 426 (1956) (Supreme Court of the United States); *See* Henry J. Friendly, *Fifth Amendment Tomorrow*, Vol. 37, U CIN. L. REV., 695 (1968).
[67] Nandini Satpathy, *supra* note 54, ¶46.
[68] Selvi, *supra* note 48, ¶126.
[69] Hiibel v. Sixth Jud. Dist. Ct. of Nev., 542 U.S. 177 (2004) 189 (Judicial District Court of Nevada, Humboldt City).
[70] *See* Selvi, *supra* note 48, ¶130; Nandini Satpathy, *supra* note 54, ¶47.
[71] Hoffman, *supra* note 65, 487.
[72] Doe v. United States, 487 U.S. 201 (1988) 213 (Supreme Court of the United States); Miranda v. Arizona, 384 U.S. 436 (1966) (Supreme Court of the United States); Counselman v. Hitchcock, 142 U.S. 547 (1892) (Supreme Court of the United States).

akin to the position in India, wherein physical evidence such as a blood sample,[73] a handwriting sample,[74] or even a demonstration of wearing an article of clothing[75] is not a testimonial act since it does not compel the accused to be a "witness.".

Thus, both jurisdictions rely on the same foundational principles on the right against self-incrimination for both jurisdictions, making a comparative analysis viable. Admittedly, the one crucial difference lies in their approaches towards illegally obtained evidence or "fruit of the poisoned tree", the implications of which will be mitigated in Part V of the paper.

IV. THE FOREGONE CONCLUSION DOCTRINE

This part of the paper first explores the development of the Foregone Conclusion Doctrine in the U.S. through case laws. In doing so, it highlights two primary schools of thought that emerged and scholarly debates on the same. Ultimately, with privacy and the right against self-incrimination as the foremost concern, the paper picks a side to corroborate, while the next part argues for its application in the Indian context.

A. A TRADITIONAL UNDERSTANDING OF THE FOREGONE CONCLUSION DOCTRINE

The current legal puzzle surrounding data encryption and the government's power to investigate encrypted data is whether the government can force an individual to unlock the device by providing them with the password or code with which the device has been encrypted.[76] In other words, how much power does the government have to compel a person to decrypt a device by entering a password? On this question, courts have not reached a conclusive answer, and scholars have also presented diverging views.[77]

The Doctrine of Foregone Conclusion propounded in the U.S. in *Fisher* v. *United States* ('Fisher'), states that if the government knows exactly what evidence it is looking for in a criminal investigation, then the act of unlocking a device to obtain that evidence is not a violation of self-incrimination since the act of opening the phone is a "foregone conclusion''.[78] The fact is, there was only one sentence in Fisher which led to the eventual unpacking of the Foregone Conclusion Doctrine in U.S. jurisprudence.[79] Moving forward, to demonstrate the contradictory stance of U.S. courts, the paper will analyse two conflicting cases from the Supreme Courts of Pennsylvania and New Jersey, to ultimately reach a principle which centres on the right against self-incrimination, as seen in India.

---

[73] Schmerber v. California, 384 U.S. 757 (1966), 765 (Supreme Court of the United States).
[74] United States v. Euge, 444 U.S. 707 (1960), 716-18 (Supreme Court of the United States).
[75] Holt v. United States, 218 U.S. 245, (1910), 252–53 (Supreme Court of the United States).
[76] *In re* Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1349 (11th Cir. 2012) (Court of Appeals for the Eleventh Circuit) ('Grand Jury Subpoena') (declaring that the government could not compel decryption); United States v. Apple MacPro Computer, 851 F.3d 238, 248 & n.7 (3d Cir. 2017) (United States Court of Appeals, Third Circuit) (allowing compelled decryption).
[77] As Professor Sacharoff has recently explained, this is a "fundamental question bedevilling courts and scholars", *see* Laurent Sacharoff, *Unlocking the Fifth Amendment: Passwords and Encrypted Devices*, Vol. 87(1), FORDHAM L. REV., 207 (2018) ('Sacharoff Fordham').
[78] Fisher v. United States, 425 U.S. 391 (1976), 411 (Supreme Court of the United States) ('Fisher').
[79] *Id*., 411 (The sentence read as: "[t]he existence and location of the papers are a foregone conclusion and the taxpayer adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers").

The Supreme Court of Pennsylvania, in *Commonwealth* v. *Davis* ('Davis'),[80] dealt with an administrative subpoena which was sent to the defendant, Joseph Davis, to intercept child pornography sent to his Internet Protocol ('IP') address.[81] Davis admitted in police custody that he was the "sole-user" of the password protected computer and knew its password.[82] He also admitted to watching pornography involving minors on the device and claimed to not understand why the same was illegal in the U.S.[83] Ultimately, the Court laid down the requirement that compelled electronic device decryption can only occur when the government can establish first, the existence of the evidence demanded, second, possession of the evidence by the defendant, and third, the authenticity of the evidence.[84]

Meanwhile, the Supreme Court of New Jersey, in *State* v. *Andrews* ('Andrews'),[85] applied the "act of production doctrine", asserting that the State's knowledge of the passcodes made the disclosure a "foregone conclusion". From this case, the exception pertains solely to the passcode itself, making it more feasible for the government to satisfy the burden associated with the foregone conclusion exception. Thus, when the government knows, first, the password exists, second, the suspect possesses it, and third, it is authentic, the testimonial value is "minimal", then the government can ask the person to unlock their phone.[86] Simply put, while Andrews centred its inquiry on the password, Davis did it on the contents of the device itself.

Notably, a view similar to Davis was postulated in In re Subpoena Duces Tecum, where the court concluded that the Doctrine would apply only "if the Government can show with 'reasonable particularity' that, at the time it sought to compel the act of production, it already knew of the materials".[87] Diverging opinions of U.S. courts on the application of the Foregone Conclusion Doctrine fail to establish a settled position of law, necessitating further inquiry through the usage of scholarly opinion.

B. PASSWORDS AS AN INVESTIGATIVE TOOL

As shown above, the jurisprudence on the Foregone Conclusion Doctrine is murky and often contradictory. Scholars on the subject have advanced their understanding of the Doctrine, and their arguments are worth consideration.

The two different views on this aspect are concerning knowledge of the government, which they ought to have regarding the contents and passwords before ordering the person to unlock the phone. One school (led by Orion Kerr) endorses the view that the government should know that the person knows the passwords, and this mere knowledge makes it a foregone conclusion that the contents of the device are also known to the person who knows the password. The other view (led by Laurent Sacharoff) states that the government ought to have reasonable belief that there is some incriminating material in the person's phone, and only then can they make the person unlock their device.

---

[80] Commonwealth v. Davis, 220 A.3d 534, (Pa. 2019) 549, 551 (Supreme Court of Pennsylvania Middle District) ('Davis').
[81] *Id*., 537.
[82] *Id*., 538.
[83] *Id.*
[84] *Id*.
[85] State v. Andrews, 234 A.3d (N.J. 2020), 1254 (Supreme Court of New Jersey).
[86] Norman Hobbie Jr., *Reconsidering the Foregone Conclusion Doctrine- Compelled Decryption and the Original Meaning of Self-Incrimination*, Vol. 20(1), UNI. OF NEW HAMPSHIRE L. REV., 82 (2021).
[87] Grand Jury Subpoena, *supra* note 76, 1346.

The leading authority in this regard, Orin Kerr, believes that the Fifth Amendment does not pose any barrier for the government to investigate a person's device if the government knows that this particular individual is aware of the password by which the device has been encrypted.[88] He posits that there is an inherent presumption that if an individual possesses knowledge of a device's password, they possess knowledge of its contents.[89] However, as pointed out by Professor Laurent Sacharoff, this analysis of Kerr and the rule he postulated seems to contradict precedent.[90] Sacharoff proposes a test opposite to what was argued by Kerr and endorses a similar view as propounded in In re Grand Jury Subpoena Duces Tecum.[91] He argues that the government must obtain prior knowledge of an individual's possession of files on a device and accurately identify these files with a fair level of specificity.[92]

At this stage, the theoretical foundations of the two schools are worth discussing. The Fourth Amendment to the U.S. Constitution protects people from unreasonable search and seizures by giving them the right to be secure in their "persons, houses, papers and effects".[93] Sacharoff characterises the overlap between the Fourth and Fifth Amendment as one which warrants harmonising.[94] While the Fourth Amendment gives an investigating officer access to all the information on the device, the Fifth Amendment gives the accused the right to remain silent and thus denies access to the same data.[95] To resolve this, Sacharoff claims to draw his rule of particularity from the "best principles" of the Fourth and Fifth Amendments to the U.S. Constitution.[96] Sacharoff claims to uphold the Fifth Amendment by protecting the accused from making his entire "digital life available" and thus assisting in his own prosecution.[97] The rule also protects the crux of the Fourth Amendment, which is, informational privacy,[98] by limiting state access to exploratory searches which could expose the accused to new charges.[99]

On the other hand, Kerr postulates that when the government compels acts (in this case, decrypting a device), instead of words (such as answering a question), the purpose of compelling acts is to obtain evidence that the act itself can reveal.[100] Thus, if the government can independently prove the accused's knowledge of the password, the resulting data is a foregone conclusion and thus non-incriminatory in nature.[101] Kerr's interpretation of the Doctrine stems directly from Fisher which asks the question of whether what is implied in the testimony is "in issue" or if obtaining it "adds little or nothing to the sum total of the

---

[88] Orin Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, Vol. 97, TEXAS L. REV., 787 (2019) ('Kerr').
[89] *Id.*
[90] Grand Jury Subpoena, *supra* note 76, 1346; *See* Laurent Sacharoff, *What Am I Really Saying When I Open My Smartphone? A Response to Orin S. Kerr*, Vol. 97, TEX. L. REV. ONLINE, 63 (disagreeing with Kerr's definition and application of the foregone conclusion rationale) ('Sacharoff').
[91] *Id*., 64.
[92] *Id.*, 63, 64 ("Rather, the rule should be whether the government already knows the person possesses the files on the device and can identify them with reasonable particularity."); *But see* Kerr, *supra* note 88, 786–787 (criticising the Eleventh Circuit's reasonable particularity approach as unclear and, if read that way, the analysis as incorrect).
[93] The Constitution of the United States of America, 1789, Amendment IV.
[94] Sacharoff Fordham, *supra* note 77, 206.
[95] *Id*.
[96] *Id*., 208.
[97] *Id*.
[98] Eric Schnapper, *Unreasonable Searches and Seizures of Papers*, Vol. 71, VA. L. REV., 873 (1985).
[99] Sacharoff Fordham, *supra* note 77, 208.
[100] Kerr, *supra* note 88, 777.
[101] *Id*., 783.

Government's information".[102] The rule that Kerr obtains from this is that by entering the correct password, the implied testimony is neither in issue, nor adds anything to the Government's existing information since the government already knows that the accused knows his password. Thus, the testimony is a foregone conclusion, and the privilege against self-incrimination cannot apply.[103]

Significantly, Kerr's doctrinal explanation for his view, and a direct counter to what Sacharoff proposes, is that technological expansion "is a Fourth Amendment problem rather than a Fifth Amendment problem".[104] Kerr argues that technological expansion merits a response from the Fourth Amendment rather than the law on self-incrimination by characterising the respective purposes of the amendments differently. As argued by Kerr in his other works as well,[105] the way the Fourth Amendment functions is by having a sliding scale on the burden the government should fulfil to find certain information.[106] In contrast, in the context of the Fifth Amendment, the increased value of the data found by decrypting the device leaves the testimony implicit in unlocking the device unchanged. In essence, while the Fourth Amendment functions on a sliding scale, Kerr argues, the Fifth Amendment "generally acts as an absolute barrier to government access rather than a sliding scale of regulation".[107] In creating this distinction, he also claims to solve the complaint of law enforcement officials that complex encryption tools threaten public harm by thwarting criminal investigations.[108]

Kerr's interpretation and application of Foregone Conclusion Doctrine is argued to be riddled with fallacies.[109] Sacharoff argues that Kerr's approach faults by incorrectly identifying what the act of unlocking a phone communicates.[110] Unlike Kerr, Sacharoff postulates that opening a device communicates possession and knowledge of its files.[111] Thus, if the act of decryption implicitly communicates knowledge and possession, the government, to correctly apply the Foregone Conclusion Doctrine must fulfil the particularity requirement.[112]

However, stronger support for the paper rejecting Kerr's approach lies not in its technical irregularities but in Kerr's endorsement of unbounded governmental jurisdiction to enforce decryption only through password knowledge, which disregards the tangible risks associated with unregulated state authority. As correctly pointed out by Sacharoff, if Kerr's rule was to be followed, once a suspect has been compelled to unlock his device, the government has virtually no limits on the resulting search and can look at every file, folder, metadata, location and data the suspect may not even realise exists on his device.[113] This poses a potential threat of compromising personal freedoms in favour of efficiency in the context of criminal inquiries, establishing a precarious precedent.

---

[102] *Id*., 782; Fisher, *supra* note 78, 411.
[103] Kerr, *supra* note 88, 783.
[104] *Id*., 797.
[105] *See* Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, Vol. 48 (1), TEX. TECH. L. REV. (2015).
[106] Kerr, *supra* note 88, 797.
[107] *Id*.
[108] *Id.*
[109] *See* Evan Kennedy, *Protecting the Fifth Amendment: Compelled Decryption in Indiana*, Vol. 54, INDIANA L. REV., 707 (2022).
[110] Sacharoff, *supra* note 90, 68.
[111] *Id*.
[112] *Id*., 72.
[113] *Id*.

Given the implications of Kerr's argument, the paper corroborates the rule particularly laid down in Davis and championed by Sacharoff. At the same time, it acknowledges that knowledge, in the form of an implicit acceptance by the accused that the incriminating material exists on his device, is an incredibly high burden to meet. Perfect knowledge of the exact files that the government seeks as evidence can only be born out of cases with peculiar circumstances. As mentioned earlier, in Davis, the accused admitted multiple times that he regularly watched pornographic content, particularly that involving minors.[114] It was after this statement by the accused that the court concluded that compelled disclosure of the password would not reveal to the court anything that they did not already know.[115] Thus, the foregone conclusion exception was successfully applied.

The next part of the paper lays down the viability of the Foregone Conclusion Doctrine in India, and the part subsequent to it lays down a justification for why, given the nature of cell phones, a high threshold to compel decryption is necessary to protect privacy rights.

V. ADOPTION OF THE FOREGONE CONCLUSION DOCTRINE IN INDIA- VIABILITY AND CHALLENGES

There has been no formal acknowledgement or adoption of the Foregone Conclusion Doctrine in India's limited jurisprudence on digital evidence so far. While Mahesh Kumar Sharma correctly prohibited the compelled decryption of an electronic device, the Foregone Conclusion Doctrine aims to create a narrow exception to this general prohibition that can aid criminal investigations. This part first argues that, on analysing the recent petitions before the SC to lay down guidelines for the seizure of electronic devices, there seems to be scope for the emergence of a limited version of the Foregone Conclusion Doctrine in India. Thereafter, as an impediment to its successful application in the future, the next part recognises the problem in Mahesh Kumar Sharma by treating biometrics and passwords differently.

A. DIRECTION TO ISSUE GUIDELINES ON SEIZURE OF ELECTRONIC DEVICES

In November 2023, in the aftermath of Virendra Khanna, the SC agreed to hear a writ petition seeking guidelines on the seizure of electronic devices by investigating agencies.[116] While the SC directed the government to "lay down inviolable guidelines", it cautioned that the law in this regard must have "adequate safeguards" to protect fundamental rights and the right against self-incrimination. Ultimately, while these guidelines are yet to be formed, the government assured the Court that until interim guidelines were passed, the 2020 CBI (Crime) Manual on Digital Evidence would be followed.[117]

Of relevance here are the specific suggestions on search of electronic devices as argued in the petitions *Ram Ramaswamy* v. *Union of India* ('Ram Ramaswamy')[118] and

[114] Davis, *supra* note 80, 538.
[115] *Id*.
[116] Ram Ramaswamy and Ors. v. Union of India, W.P. (Crl) No. 138/2021.
[117] Radhika Roy, *Union Government Assures the SC that Procedure in CBI Manual will be followed in Search and Seizure of Digital Devices before Guidelines are Formed,* INTERNET FREEDOM FOUNDATION, December 18, 2023, available at https://internetfreedom.in/sc-search-seizure-union-guidelines-cbi-manual-dec/ (Last visited on May 29, 2024).
[118] Ram Ramaswamy and Ors. v. Union of India, W.P. (Crl) No. 138/2021.

Foundation for Media Professionals v. *Union of India* ('Foundation for Media Professionals').[119]

The suggested interim guidelines in both instances lay down the requirement of a judicial warrant for seizure of electronic devices, with the exception of emergency searches.[120] Specifically, they suggest that such application for warrant must not "be in the nature of a roving and fishing inquiry and must, in specific terms, set out the nature of information that the law enforcement agency expects to find and secure on the device".[121] Seizure on the "conjecture that evidence 'may' (emphasis added) be found" will be impermissible in all circumstances.[122] The four-fold test laid down in Ram Ramaswamy in this regard is as follows — "d. Whether it contains evidence, in which case, the precise nature of the thing that is sought as evidence, the basis for suspecting that the same will be found in the device, and its relevance to the case must be specified".[123]

If adopted, the implication of these guidelines is significant insofar as investigation agencies will be required to establish the existence, the basis for suspecting this existence, and the relevance of the evidence to the case, showing that there is a limited adoption of the Forgone Conclusion Doctrine. While admittedly, the threshold is not as high as the Doctrine, at least at this preliminary stage, it is the right step in finding the balance between giving unfettered access to devices to investigation agencies and rendering the contents of an electronic device obsolete for the purposes of criminal investigation. For the Davis particularity argument to be met, the guidelines laid down by the State must go a step beyond the recommendation in the petition to require the investigating agency to know the authenticity of this sought-after evidence on the accused's device as well, beyond merely looking at the link with the offence.

The process of retention of relevant material is also worth discussing. Ram Ramaswamy proposes extensive guidelines to ensure that the investigating officer has access only to the evidence, the existence, and relevance of which has been detailed in the search warrant. First, Ram Ramaswamy proposes examination by an independent agency, wherein the presence of the accused, all privileged and irrelevant material, is identified and a copy of only the relevant material is taken.[124] The independent investigating agency is barred from accessing or disclosing to the investigating officer, any irrelevant or privileged material "to the extent the same comes to its notice accidentally or otherwise".[125]

The requirement for material irrelevant to the investigation to be removed in the presence of the accused largely mitigates the concerns laid down in Mahesh Kumar Sharma. The Delhi Sessions Court in Mahesh Kumar Sharma distinguished between the U.S. and Indian law on evidence insofar as while in the U.S., illegally obtained evidence is prohibited from being used in any case, while in India the same can be presented before a court under limited circumstances.[126] Thus, the Court concluded that if in decrypting a device certain information was revealed which was incriminating, the same would have to be used against the accused.[127]

---

[119] Foundation for Media Professionals v. Union of India, WP (Crl) No. 395/2022 ('Foundation for Media Professionals').
[120] *Id*., ¶51; Ram Ramaswamy and Ors. v. Union of India, W.P. (Crl) No. 138/2021, *Suggested Interim Guidelines filed by the Petitioner*, ¶1 ('Ram Ramaswamy Interim Guidelines').
[121] Foundation for Media Professionals, *supra* note 119, ¶51.
[122] Ram Ramaswamy Interim Guidelines, ¶3.
[123] *Id*., ¶2(d).
[124] *Id*., ¶9.
[125] *Id*.
[126] Mahesh Kumar Sharma, *supra* note 3, ¶39.
[127] *Id.*

The argumentation of the paper so far attempts to solve the first step of this conundrum by arguing for adoption of the Foregone Conclusion Doctrine. If the investigating agency is aware of the existence and authenticity of the sought-after evidence, its existence is a foregone conclusion, and it no longer incriminates the accused. As for the risk of other incriminating material being found on the device incidental to its decryption, the above-quoted guidelines remedy that by asking for all data irrelevant to the investigation to be deleted in the presence of the accused. Thus, these suggested guidelines, if adopted, are a step in the right direction and also mitigate the concerns raised in Mahesh Kumar Sharma.

The acknowledgement by Ram Ramaswamy of the independent agency accidentally stumbling across personal material and mandating its deletion instead of handing it over to the investigating officer is imperative. Cases like these are not a rarity and the practical significance of this guideline is demonstrated by the In Re Boucher case where the police noticed certain images on the defendant's computer before he could close it.[128] Thereafter, the police could not access the files without a password and obtained a subpoena to compel decryption.[129] The Court rejected the plea by the defendant that requiring him to produce unencrypted versions of the files would incriminate him to hold that since law enforcement had already seen the files, they were a foregone conclusion.[130] The order by the Court to produce 'all' documents on the device, as opposed to just the ones that the police had seen before the accused closed his device has been correctly criticised by commentators.[131] The particularity requirement was only fulfilled for those documents the government had seen on the unlocked device, not the entirety of information present on the device.

As per the recommendations in the petitions above, by first, preventing an exploratory search, and second, routing the phone to an independent agency which will make a copy and send it to the investigating officer prevents irrelevant and possibly incriminating material from being used against the accused.[132] Thus, in cases where the particularity requirement is met, these guidelines constitute a positive framework which the paper advocates for, in addition to the prohibitions laid down in Mahesh Kumar Sharma. Admittedly, this suggestion only works if investigation agencies are sensitised to the particularity requirement, an eventual goal which the paper nonetheless advocates for.

Thus, while yet to be adopted by courts, the Foregone Conclusion Doctrine seems to be compatible with Indian law on self-incrimination.

B. HARMONISING THE LAW ON COMPELLING BIOMETRICS AND PASSWORDS

As discussed, Virendra Khanna was succeeded by Mahesh Kumar Sharma, which apart from holding the former to be *per incuriam*, also refuted it specifically on the point of treating passwords and biometrics in the same manner. Mahesh Kumar Sharma held that since compelled disclosure of passwords required the "personal knowledge of the accused",[133] while the collection of biometrics is a largely "mechanical process",[134] an accused can be asked

[128] In re Grand Jury Subpoena to Sebastien Boucher, No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009) (United States District Court for the District of Vermont).
[129] *Id.*, 2.
[130] *Id.*, 4.
[131] *See* Sacharoff Fordham, *supra* note 77, 235.
[132] *See* Ram Ramaswamy Interim Guidelines, ¶9(viii).
[133] Mahesh Kumar Sharma, *supra* note 3, ¶27.
[134] *Id.*

to give his biometrics but cannot be asked to give his password for the purposes of unlocking his phone.

The paper argues that Mahesh Kumar Sharma errs in its logic insofar as it creates an artificial distinction between compelling disclosure of a password and compelling a person to give their biometrics to unlock a device. While admittedly, this distinction between 'physical evidence' and 'testimonial evidence'[135] is drawn from the Criminal Procedure (Identification) Act, 2022 ('Act'), it merits serious reconsideration since, irrespective of the method employed, the outcome in both circumstances is the same — unlocking the device of the accused.

The applicability of the Act in this context is also questionable. The Act replaces the Identification of Prisoners Act, 1920, and allows for the collection of identifiable information from, *inter alia*, convicts to expedite their identification and future investigation.[136] Notably, the Act applies to convicts, arrestees, and those ordered to give security for maintaining peace under §117 of the CrPC.[137] As correctly held in Mahesh Kumar Sharma, "measurements" under the Act include biometric information such as fingerprints and retina scans.[138] The Court goes on to note that since the Act does not apply to a password of an electronic record, the accused cannot be compelled to produce the same.[139] This reasoning by the Court is absurd since first, the goal of the Act, which is to keep a record of convicts and arrested persons for easy identification is entirely different from the scenario of self-incrimination the court deals with in Mahesh Kumar Sharma, which involves witnesses and deals with the investigation and trial of offences. Second, as discussed previously, the Act only applies to convicts and arrestees and does not apply to accused individuals at all. Thus, notwithstanding the critique of the Act itself, a legislation aimed at keeping a record of convicts and arrested persons cannot be transplanted to the investigation of an accused.

In any case, the primary argument the authors make is that any future analysis undertaken by courts in India in this regard necessarily needs to be outcome-determinative instead of focusing on the form of decryption. In 2017, the U.S. District Court in the Northern District of Illinois discussed whether law enforcement agencies can compel biometrics from an accused.[140] In applying previous U.S. Supreme Court decisions, the District Court held that the compelled act of using one's biometrics does "explicitly or implicitly relate a factual assertion or disclose information", since through unlocking the phone using say, one's fingerprints, the suspect is testifying, at minimum, that they have accessed the phone before to set up the password and thus have some level of control over the device.[141]

The act of compelling biometrics cannot be seen in isolation from the result it produces, i.e., unlocking a digital device. The solution the paper proposes is that while the general dictum in Selvi can be maintained, and using biometrics such as fingerprints need not amount to testimonial compulsion, this position necessarily needs to be deviated from when the biometrics are used for the production of additional information; in this case, the contents of a formerly locked electronic device. If the biometrics do unlock the device, the accused concedes, at minimum, access to the phone in its unlocked form to configurate the phone to

[135] *Id*., ¶29.
[136] The Identification of Prisoners Act, 1920.
[137] The Criminal Procedure (Identification) Act, 2022, §4.
[138] *Id*., §2(b).
[139] Mahesh Kumar Sharma, *supra* note 3, ¶26.
[140] *See* In re Search Warrant Application for [Redacted Text], 279 F. Supp. 3d 800, 804 (N.D. 111. 2017) (United States District Court, N.D. Illinois, Eastern District).
[141] *Id.*, 1073.

recognise his fingerprint. Thus, "the seemingly non-testimonial physical characteristic is made testimonial because of the way the characteristic is being used".[142] It needs to be clarified at this juncture that in this argument, compelling biometrics is permitted in case the requirements of the Foregone Conclusion Doctrine are met. If the law enforcement agency can anticipate the full contents of the device and is cognisant of its authenticity, the biometrics, like a numerical or alphabetical password becomes a foregone conclusion.

The prevailing position among consumers as well as from a data security perspective, seems to be that biometrics are preferable to passwords since they store their data in a secured "non-reversible" algorithm.[143] A study by Visa conducted in 2018, albeit in the context of online transactions, concluded that 99 percent of respondents were interested in using at least one biometric to verify their identity or make online payments.[144] Given the rampant use of biometrics in India, compounded by a general lack of awareness of the law, it is imperative for judgments subsequent to Mahesh Kumar Sharma to consider widening the ambit of the prohibition on decryption of devices to include compelling biometrics as well.

VI. WHY CELLPHONES WARRANT THE CREATION OF A NEW ZONE OF PRIVACY

A necessary implication of the argument we adopt is that cell phones warrant the creation of an entirely new, impenetrable zone of privacy akin to the human mind. In Virendra Khanna, the Court was acutely aware that once an investigating agency has access to an electronic device, particularly a cell phone, they would have "free access" to all data, not only on the said equipment but also of cloud services related to the equipment which would inevitably include personal details and "privileged communications".[145] The court concluded without explanation that the use of such data would not amount to a violation of privacy and fall under the exceptions carved out in *K.S. Puttaswamy* v. *Union of India* ('Puttaswamy').[146] An assertion that aided the court in holding this is that the rules that are applicable to physical documents containing privileged communication cannot apply to cell phones or electronic devices with the equivalent information.[147]

While this part of the ruling will be addressed in the portion on the third-party doctrine, we argue that the way the Court characterises cell phones as devices which warrant limitless intrusion by law enforcement agencies is fundamentally problematic. This portion largely makes use of U.S. jurisprudence, since equivalent cases which discuss the encroachment of cell phones in everyday life and its privacy implications do not exist in Indian jurisprudence yet.

The case of *Ontario* v. *Quon*[148] involved the reasonable expectation of government employees to have their text messages sent on employee-owned pagers be kept

[142] In re Search of a Residence in Oakland, Cal., 354 F. Supp. 3d. (N.D. Cal. 2019) 1016 (United States District Court, Northern District of California).
[143] Allesandro Mascellino, *Why Biometrics are Better than Passwords?*, BIOMETRIC UPDATE, August 30, 2022, available at https://www.biometricupdate.com/202208/why-are-biometrics-better-than-passwords (Last visited on May 29, 2024).
[144] INDIAN EXPRESS, *Indian Consumers Favour Biometric Authentications Over Passwords*, January 18, 2022, available at https://indianexpress.com/article/technology/tech-news-technology/indian-consumers-favour-biometrics-over-passwords-visa-5028580/ (Last visited on May 29, 2024).
[145] Virendra Khanna *supra* note 1, ¶15.2.
[146] *Id*., ¶15.5.
[147] *Id*.
[148] Ontario v. Quon, 560 U.S. 746 (2010) (Supreme Court of the United States).

private. Here, U.S. Supreme Court acknowledged as early as 2010 that given their pervasive nature, cell phone conversations are "necessary instruments for self-expression, even self-identification".[149] The identification of cell phones as devices warranting a higher level of protection was seen most clearly in the case of *Riley* v. *California*[150] which created the cornerstone of data protection in the U.S., by requiring investigating agencies to furnish a warrant before a government searches a phone for its data. In reaching this conclusion, the court marvelled at the indispensable nature of cell phones as a part of daily life so much so that they may be called "an important feature of human anatomy".[151] This link with human anatomy is important because it shifts the focus away from the device to the mind of the individual. This renders debates about the 'property aspect' of privacy moot. If cell phones are indeed an extension of the human mind, the proposed idea does not create a new sphere of privacy but extends the applicability of the right over a region already recognised as inviolable, i.e., the human body. Later, in *Carpenter* v. *United States* ('Carpenter'),[152] the Court held that the "retrospective quality" of data in a mobile phone gives the police access to data which is "otherwise unknowable".

Cell phones are dynamic in nature, described by Bryan Choi as "always-in-use devices".[153] An unlocked cell phones reveals the applications used by the user, the notifications received by them in real-time and in some cases, even their location. This is compounded by the fact that given its ubiquity, a multitude of cell phone users are unaware of restrictive privacy settings on their devices, rendering their intimate information vulnerable in a decrypted device.[154] The perpetually dynamic nature of a cell phone is precisely what distinguishes it from say, a physical folder of confidential documents. The former contains evidence which is sequestered in a device, which is wired to document every move that the user makes on it. This part of the paper limits its argumentation to cell phones since no other electronic device has achieved that level of intimacy with its owner's cognitive engagement. As put succinctly by Choi, data inside a cell phone, chosen to be kept there to maintain its private nature, can cause no more harm to the world than an "idle murderous thought".[155] In fact, idle thoughts seen in the form of notes or text communications on a cell phone are 'unpublished' thoughts that law enforcement agencies should not have access to. Scholars argue that the right to freedom of speech should extend to externalising one's mental contents in a way that one wants to, and there must be protection from interferences which "disrupt or disable the operation of these processes".[156]

On principle, while we argue that cell phones warrant the same level of protection as the human mind, this idea, to be effective, must extend to the 'method' of surveillance adopted by investigation agencies as well. The subsequent part of the paper will explore this idea with reference to the third-party doctrine. Discussion on the third-party doctrine is significant since it extends the analysis of the paper to information that is present on a cell phone 'via' cloud services, specific applications like email accounts and the internet

[149] *Id.*
[150] Riley v. California, 134 S. Ct. 2473 (2014) (Supreme Court of the United States) ('Riley').
[151] *Id.*, 2484.
[152] Carpenter v. United States, 138 S. Ct. 2206 (2018) (Supreme Court of the United States) ('Carpenter').
[153] Bryan H. Choi, *The Privilege Against Cellphone Incrimination*, Vol. 97, TEXAS L. REV., 75 (2019) ('Choi').
[154] *See* ACM DIGITAL LIBRARY, *Users' Expectations About and Use of Smartphone Privacy Settings*, April 2022, available at https://dl.acm.org/doi/fullHtml/10.1145/3491102.3517504 (Last visited on October 25, 2023) (A survey by the authors also suggests that minority groups disproportionately struggle with technological comprehension).
[155] Choi, *supra* note 153, 79.
[156] Seana Valentine Shiffrin*, A Thinker-Based Approach to Freedom of Speech*, Vol. 27(2), CONST. COMMENT., 285, 294 (2011).

browser. Evidence obtained by these means was specifically delineated in Virendra Khanna as being significant to criminal investigations.[157] India's position on the third-party doctrine is discussed to demonstrate that investigation agencies cannot be given the latitude to say, search a person's text messages merely because the evidence is hosted on a third-party platform such as WhatsApp.

VII. THIRD-PARTY DOCTRINE - CREATING A FRAMEWORK IN LIGHT OF INDIAN PRINCIPLES

The third-party doctrine, as developed in U.S. jurisprudence, states that there can be no expectation of privacy in information voluntarily provided to others.[158] Scholars argue that the element of voluntary disclosure, which is essential to the third-party doctrine, cannot apply to modern technology since carrying a cell phone and subsequently, utilising social media is no longer a meaningful choice, but "indispensable to participation in modern society".[159]

In this context, this part first discusses the development of the doctrine in the U.S. and its eventual weakening through case law. Subsequently, India's rejection of the doctrine is discussed to strengthen the conclusion of the paper, that individuals retain their reasonable expectation of privacy even in information voluntarily disclosed to social media applications such as WhatsApp.

A. THE THIRD-PARTY DOCTRINE AND ITS APPLICATION TO SEARCHES

At this stage, it is necessary to anticipate a primary objection which might arise to the paper's argumentation. It might be argued, particularly in the context of communication with third-party intermediaries through text messages and emails, that since individuals consensually host themselves on these platforms, they forfeit their expectation of privacy in this regard. The applicable IT Rules use a wide net to define social media intermediaries as intermediaries which "enable(s) online interaction between two or more users" by allowing them to create, upload or access information using its services.[160]

Immortalised in the case of *Smith* v. *Maryland* ('Smith'), the third-party doctrine encapsulates the idea that once individuals voluntarily give up their information to a third party, they assume the risk of unauthorised disclosure.[161] The court held in Smith that the government's use of a pen register, which was used to record outgoing phone numbers was not an impermissible 'search' since people do not entertain any expectation of privacy in the numbers they dial.[162] Similarly, in *United States* v. *Miller* ('Miller'),[163] while investigating Miller for tax evasion, the government obtained several months' worth of Miller's cheques and monthly statements and rejected his plea to suppress the financial records under the Fourth Amendment. In doing so, it held that Miller could "assert neither ownership nor possession" since they were "negotiable instruments to be used in commercial transactions."[164] Thus, "in

[157] Virendra Khanna, *supra* note 1, ¶8.11.
[158] United States v. Miller, 425 U. S. 435 (1976) 443 (Supreme Court of the United States) ('Miller').
[159] Carpenter, *supra* note 152, 2220; Grade Manning, *Alexa: Can You Keep a Secret? The Third-Party Doctrine in the Age of the Smart Home*, Vol. 56, AMERICAN CRIMINAL L. REV. (2019).
[160] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, R. 2(1)(w).
[161] Smith v. Maryland 442 U. S. 735, 741 (1979) (Supreme Court of the United States) ('Smith').
[162] *Id*., 742
[163] Miller, *supra* note 158, 435.
[164] *Id*., 440.

revealing his affairs to another", the defendant had assumed the risk of conveying information to the government.[165]

It was only in 2018 in Carpenter[166] that the U.S. Supreme Court recognised the inapplicability of the doctrine in a world where nearly all data, voluntarily or involuntarily, was disclosed to third parties. In relation to Cell-Site Location Information ('CSLI'), which would form every time a cell phone interacted with a cell site, the Court held that there existed a reasonable expectation of privacy and in no way does a user "assume the risk" of turning over a comprehensive dossier of his physical movements.[167] The threshold in Carpenter was correctly recognised by the court to be even higher than cases involving GPS monitoring of vehicles, since while individuals regularly leave their vehicles, they "compulsively" carry their cell phones with them everywhere. Significantly, Carpenter extended the application of the doctrine to an entirely new set of information which is exceedingly relevant in contemporary times.

B. IMPLICIT REJECTION OF THE THIRD-PARTY DOCTRINE IN INDIA

At this stage, it is pertinent to explore India's position on the doctrine, particularly in light of Virendra Khanna's assertion that rules which are applicable to a physical document which contains privileged communication cannot be applied to "data which is stored on a smartphone or any other electronic equipment."[168]

The Indian position on the third-party doctrine is significant since it lays down a foundation for an expansive reading of privacy, arguably even wider than what Carpenter held. In the case of *District Registrar and Collector, Hyderabad* v. *Canara Bank* ('Canara Bank'),[169] in revising a position of the Indian Stamp Act, 1899,[170] relating to searches, the SC notably held that privacy is a right which is attached to people and not places.[171] The Court categorically cited extensive criticism of Miller,[172] and used the test for "reasonable expectation of privacy" as laid down in *Katz* v. *United States*.[173]

The primary dicta laid down in Canara Bank was that since privacy belongs to "persons and not places", documents of a person which is in a bank should continue to be shielded by confidentiality "even if they are no longer at the customer's house and have been voluntarily sent to a bank.[174] By making the individual the centre of its inquiry, the crux of Canara Bank is that the nature of documents *vis a vis* the individual remains unchanged, even if they undergo a locational shift which might be entirely voluntary.

While Canara Bank involves the Indian Stamp Act, and Virendra Khanna addresses digital evidence, the privacy principles established in Canara Bank have broader applicability. It is argued that Canara Bank's emphasis on privacy rights attaching to individuals rather than locations transcends the specific legal context of the Stamp Act, making it highly relevant in an era where data is frequently stored and transferred across various platforms.

---

[165] *Id*., 443.
[166] Carpenter, *supra* note 152.
[167] *Id*., 21.
[168] Virendra Khanna, *supra* note 1, ¶11.1.
[169] Canara Bank, *supra* note 57.
[170] The Indian Stamp Act, 1899, §73.
[171] Canara Bank, *supra* note 57, ¶39.
[172] *Id*., ¶48.
[173] Katz v. United States, 389 U. S. 347, 351 (1967) (Supreme Court of the United States of America).
[174] Canara Bank, *supra* note 57, ¶53.

Canara Bank's doctrine aligns with the broad privacy rights established in Puttaswamy, which recognised privacy as an intrinsic part of human dignity and autonomy.[175]

The position of privacy as seen in *M.P. Sharma* v. *Satish Chandra* ('M.P. Sharma'), was that that the only safeguards for protecting privacy in searches were those provided in 'statutes', as opposed to the Constitution.[176] Puttaswamy struck down MP Sharma insofar as it said that there was no constitutional principle to classify searches as illegal,[177] thus creating a significant constitutional threshold for the State to meet in undertaking search and seizures. In fact, the significance of Canara Bank in advancing privacy jurisprudence was acknowledged in Puttaswamy where the SC held that while the case concerned bank documents, any information provided by a person to a third party carries with it a reasonable expectation of privacy, and parting with the documents does not deprive the individual of his privacy interest.[178] Thus, emanating from the decision in Canara Bank there is a need to read "procedural safeguards to ensure that the power of search and seizure … is not exercised arbitrarily."[179]

Arguably, Canara Bank envisages a scenario even wider than Carpenter. U.S. jurisprudence on the doctrine was limited to cell-site records or call records on a pen register. Canara Bank involved relinquishment not merely of control but also voluntary changing of the location of the documents in question. It is this position that also directly contradicts the assertion made by Virendra Khanna that the rules governing physical documents cannot be transposed to electronic devices. If it is established that privacy belongs to people and not places, first, the physical manifestation of information and second, its location is immaterial.[180]

Canara Bank also cautioned that "under the garb of Section 73", the authorised person may go on a rampage searching the residence of the person, and any number of documents may be inspected, seized and removed, making the exercise of power entirely disproportionate to the aim sought to be achieved.[181] The same guiding principle of search and seizure being a "serious invasion of the privacy of a person" has led to courts adopting a strict construction of §132(5) of the Income Tax Act, 1961,[182] and §§42 and 43 of the Narcotic Drugs and Psychotropic Substances Act, 1985.[183]

If the goal is to prohibit government intrusions in all places where individuals to have a 'reasonable expectation of privacy' and privacy belongs to 'people and not places', the same rules which apply to a person's home must also apply to intangible platforms, i.e., the internet and information stored on cell phones.[184] Thus, applying this rationale to giving

[175] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1, ¶266 ('Puttaswamy').
[176] M.P. Sharma v. Satish Chandra, AIR 1954 SC 300, ¶18 ('MP Sharma') ("Nor is it possible to import that doctrine with its differentiation between legal and illegal searches into our Constitution because we have nothing in our Constitution corresponding to the Fourth Amendment enabling the courts to import the test of unreasonableness or any analogous criterion for discrimination between legal and illegal searches").
[177] Puttaswamy, *supra* note 175, ¶377.
[178] *Id*., ¶66.
[179] *Id*.
[180] *See* Virendra Khanna *supra* note 1, ¶15.5.
[181] Canara Bank, *supra* note 57, ¶59.
[182] P.R. Metrani v. CIT, (2007) 1 SCC 789; The Income Tax Act, 1961, §132(5).
[183] Directorate of Revenue v. Mohd. Nisar Holia, (2008) 2 SCC 370; The Narcotic Drugs and Psychotropic Substances Act, 1985, §§42, 43.
[184] *See* Tiffany Jung, *Reclaiming Our Reasonable Expectation of Privacy: The Case Against the Third-Party Doctrine,* COLUMBIA UNDERGRAD. L. REV. (2018), available at https://www.culawreview.org/journal/reclaiming-our-reasonable-expectation-of-privacy-the-case-against-the-third-party-doctrine (Last visited on June 5, 2024).

investigating authorities free reign to look for incriminating evidence on cell phones with biometric passwords also violates well-established principles of search and seizure in India.

In the absence of clear, positive guidelines from courts or legislation, India's position on compelled decryption cannot be seen in isolation from its vast jurisprudence of privacy and searches.

VIII. CONCLUSION

The judgment in Virendra Khanna sets us back decades in terms of privacy protection and the right against self-incrimination. While a possible overruling from the SC is probable and preferable, Mahesh Kumar Sharma is a step in the right direction. Ultimately, there needs to be some specificity in the way searches of electronic devices are undertaken. Permitting investigating authorities to compel decryption to look for certain digital evidence when they are certain that this evidence exists is an achievable balance between privacy concerns and investigative imperatives.

Technological advancement has the potential to limitlessly decrease the realm of guaranteed privacy. This technology enables the government to intrude into traditionally private areas with ease. In adapting to these developments, the goal of courts needs to be an expansion of constitutionally protected areas of privacy. Scholars describe this as 'technosocial continuity', that is, recognising that intertwining technological and social needs extend the need to protect privacy from traditional social contexts to the evolving social contexts and social norms.[185]

There is still a long way to go for India to have a comprehensive law on compelled decryption of devices which respects both individual privacy and the constitutional right against self-incrimination. The paper has attempted to analyse the existing Indian position in this regard and has provided possible solutions with reference to international jurisprudence. This topic is relevant and worth exploring.

[185] Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, Vol. 70(3), MARYLAND L. REV., 622 (2011).