The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

DIGITAL STRIP SEARCHES AND CONSTITUTIONAL SILENCES: EXAMINING DATA PRIVACY GAPS AND INVESTIGATIVE MODERNIZATION UNDER THE BHARATIYA NAGARIK SURAKSHA SANHITA, 2023

~ Bharat Narayan M

Abstract

The Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), in its intent to bring about a paradigm shift in the criminal justice system in India by incorporating the advances of technology in the investigative process, has led to an unprecedented constitutional conundrum in the context of the seizure of electronic items, which is now coming to be defined as the 'digital strip search.' While the geography of the human body is limited in terms of spatial dimensions, the seizure of an individual's smartphone allows law enforcement agencies access to the entire digital persona of an individual, which encompasses financial details, health records, biometric data, and intimate communications. The present paper contends that the indiscriminate seizure of electronic items under the BNSS is in direct contravention of the principles of 'Purpose Limitation' and 'Data Minimization' as defined in the judgment in K.S. Puttaswamy v. Union of India, which essentially results in the revival of the 'general warrant' in the digital age. The present paper undertakes an in-depth analysis of the provisions of Section 94 of the BNSS in the context of Section 185 of the same act in relation to the split in judicial opinions on the 'Crime Control' model versus the 'Due Process' model while also touching upon the implications of the provisions of the BNSS on victimology and privilege. The analysis is then taken to its logical conclusion by proposing the 'Digital Evidence Code.'

Keywords: Digital Strip Search, Bharatiya Nagarik Suraksha Sanhita (BNSS), Article 21, Article 20(3), Selective Extraction, Mobile Forensics.

I. Introduction: The Metamorphosis of Evidence and the Crisis of Privacy

Currently, the criminal justice system in India is undergoing the most comprehensive reform since the 1800s. With the implementation of the BNSS (Bharatiya Nagarik Suraksha Sanhita, 2023) commencing on July 1, 2024, the old Code of Criminal Procedure, 1973 (CrPC) is no longer in force[1]. The new BNSS, along with the Bharatiya Nyaya Sanhita (BNS) and the Bharatiya Sakshya Adhiniyam (BSA), seeks to simplify the investigation process and a justice system[2]driven by technology. The reform process was presented to the public as a move to improve the rate of conviction and incorporate digital evidence into all stages of a trial [3]. However, this reform process has exposed a constitutional silence regarding the protection of digital data during the process of search and seizure.

Back in the pre-digital age, a search of a person or a place was subject to physical constraints. The warrant's scope was restricted by the physical constraints of the material to be seized[4]. Today, a smartphone, weighing less than 200 grams for most people, serves as a container for an individual's entire world. It contains an individual's financial information, location, health records, physical attributes, Internet surfing history, and personal communications. When a smartphone is seized, a "digital strip search" of an individual's digital world is performed[5].

This phrase is more than just a metaphor. It represents a touching of the individual's mind and life that exceeds any physical or material world[6]. A physical world search may reveal the layout of the physical world, whereas a digital world search may reveal the layout of the mind. This essay will explore the balance between the sweeping powers granted by the BNSS and the individual liberties

[1] Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46, Acts of Parliament, 2023 (India) [hereinafter BNSS].

[2]See Ministry of Home Affairs, Transforming Criminal Justice System in India, https://pib.gov.in (last visited Jan. 28, 2026).

[3] *Id.*

[4] *See* Entick v. Carrington (1765) 19 Howell's State Trials 1029 (holding that general warrants are contrary to the common law

[5] Abhinav Sekhri, *The Digital Strip Search*, 13 CONST. L. SOC'Y REV. 22 (2020).

[6] *See* Orin S. Kerr, *The Next Generation of Communications Privacy Law*, 162 U. Pa. L. Rev. 373 (2014).

guaranteed by Articles 14, 19, 20(3), and 21 of the Indian Constitution. It will be argued that the current system does not possess the "substantive due process" required for the digital world.

II. The Constitutional Bedrock: Privacy, Dignity, and the Puttaswamy Mandate

The challenge to the indiscriminate seizure of digital devices begins with the landmark judgment of the Supreme Court of India in the case of K.S. Puttaswamy v. Union of India, where a nine-judge bench of the Supreme Court upheld the status of privacy as a fundamental right[7]. The judgment recognized the intrinsic value of privacy as an important attribute of the dignity and autonomy of individuals, including the digital world of information self-determination[8].

A. The Tripartite Test of Proportionality

Under the Puttaswamy judgment, the infringement of privacy by the state must satisfy a four-part test:

1. Legality: The state action must be backed by a legislative provision.
2. Legitimate Aim: The state must be motivated by a legitimate objective.
3. Proportionality/Suitability: There must be a rational nexus between the objective and the state action.
4. Necessity (Least Restrictive Means): The state must use the least restrictive means to achieve the objective.[9]

The present practice in India with regard to digital seizures includes the use of full-disk imaging, whereby the entire content of the storage media of a digital device, usually running into hundreds of gigabytes, is placed under the custody of the state, irrespective of its relevance to the particular offense for which the investigation was initiated[10]. Such a practice, at first glance, seems to be in

[7] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India).

[8] *Id.* at para 310.

[9] *Id.* at para512.

[10] Nivedita Saksena, *Mobile Forensics and the Law: A Technical Perspective*, 5 INDIAN J. L. & TECH. 45 (2021).

clear violation of the principle of Necessity. If the investigation seeks to access the financial records of an individual, there is no reason to access other non-relevant information such as private photographs or health records.[11]The BNSS fails to make a distinction between pertinent and non-pertinent information, thus allowing a general warrant to be issued, a practice that was rejected by history as a principle of the past[12].

B. Data Minimization and Purpose Limitation

The Puttaswamy judgment highlights the importance of data collection being restricted to the bare minimum required to fulfill the objective for which the data was to be collected[13]. This principle of Data Minimization and Purpose Limitation was also recognized by international conventions in the Data Protection Legislation of the General Data Protection Regulation of the European Union[14]. However, the BNSS does not adhere to this principle. The custody of the data by the police continues for an indefinite period of time, irrespective of whether the individual is convicted or whether the data was irrelevant to the case.[15]

III. Article 20(3) and the Doctrine of Mental Privacy

The extension of the privilege against self-incrimination to digital devices continues to be a major and controversial area of development in the law of evidence. Article 20(3) of the Indian Constitution provides:

"No person accused of any offence shall be compelled to be a witness against himself."[16]

---

[11] *Id.*

[12] *See* V.S. Kuttan Pillai v. Ramakrishnan, (1980) 1 SCC 264 (discussing the history of general searches in India).

[13] K.S. Puttaswamy, (2017) 10 SCC 1 at para 620.

[14] General Data Protection Regulation (GDPR), Art. 5(1)(c), 2016 O.J. (L 119) 1 (EU).

[15] Report, *supra* note 11, at 3

[16] INDIA CONST. art. 20, cl. 3.

A. The Selvi Precedent and "Testimonial Compulsion"

In the case of Selvi v. State of Karnataka, the Supreme Court recognized the doctrine of mental privacy and ruled that the use of techniques of narco-analysis and brain mapping violated Article 20(3) of the Constitution as these techniques compelled the accused to divulge information contained in the mind.[17] The Supreme Court distinguished "physical evidence" from "testimonial evidence" as the latter required a positive volitional act of the mind.[18]

The argument is that the smartphone passcode is not distinguishable from the mental content in the case of Selvi. The State, in forcing the citizen to "unlock" their digital life, is compelling the citizen to provide the key to their incrimination, thereby evading the State's burden to independently discover evidence. The State, while it is within its power to conduct searches, does not, by the same token, automatically possess the power to compel the citizen to assist the State in its search by providing the password, which is held solely in the memory[19].

B. The Biometric Dilemma

The discussion becomes more complex with the inclusion of the element of "biometrics" – the use of "Face ID" or "Touch ID" to access the smartphone. The key difference is that the passcode is "something you know" – mental, while the biometric is "something you are" – physical.[20] Some courts hold the view that, since the biometric is physical, compelling the citizen to place their finger on the scanner does not violate Article 20(3).[21] The problem with this line of reasoning is the failure to recognize the inherent link between the physical action of placing the finger on the scanner and the unlocking of the digital repository containing the citizen's mind-derived

[17] Selvi v. State of Karnataka, (2010) 7 SCC 263 (India).

[18] *Id.* at para145.

[19] *See* M.P. Sharma v. Satish Chandra, AIR 1954 SC 300 (India).

[20] *See* Sarah Brayne, *Predict and Surveil: Data, Discretion, and the Future of Policing* (2020).

[21] Virendra Khanna v. State of Karnataka, 2021 SCC OnLine Kar 5032 (India).

information. This paper argues that the line is blurred in the digital age, where the physical act of unlocking the smartphone leads to the unlocking of the testimonial content held within the smartphone.[22]

IV. Statutory Deep Dive: Investigative Powers under the BNSS, 2023

The BNSS explicitly integrates digital terminology, yet it fails to provide the procedural safeguards necessary to limit the scope of digital searches.

A. Section 94: Expansion of the Summons Scope

Section 94 of the BNSS (replacing Section 91 of the CrPC) allows courts or police officers to direct the issuance of a summons for "the production of any document or electronic communication, including communication devices, which is likely to contain digital evidence.[23]" The inclusion of "communication devices" is a significant broadening of the scope of summons. By using "likely to contain," the law allows for "fishing expeditions." As all devices will have some form of digital footprint (such as location data), this provision allows for the seizure of all devices belonging to a suspect, a witness, or even a third party. Additionally, this provision does not require that the target be specific. A police officer may demand "all devices" in a home, which means that a significant amount of data may be collected from innocent family members[24].

B. Section 185: Warrantless Searches and the Myth of "Undue Delay"

Under Section 185 of the BNSS (equivalent to Section 165 of the CrPC), warrantless search is allowed if an officer has reasonable grounds to suspect that evidence is likely to be found and that there is undue delay [25]in obtaining a warrant. In the digital sphere, the condition of undue delay is always satisfied because the police can easily claim that there is undue delay in obtaining a warrant due to the risk of remote wiping of data.[26] This allows the police to carry out intrusive digital

---

[23] BNSS, Sec 94

[24] *See* Cyber Crime Cases: Issues, Challenges & Solutions, JUDICIAL ACADEMY JHARKHAND (2025).

[25] BNSS, sec 185

[26] Vrinda Bhandari, *Warrantless Smartphone Seizures: A Critique of Section 165 CrPC*, 52 ECON. & POL. WKLY. 18 (2017).

search without the need for a "neutral and detached magistrate," which is the norm in other democracies[27]. The absence of a formal procedure of obtaining a Digital Search Warrant under the BNSS implies that the scope of warrantless search is entirely in the hands of the police officer[28].

C. Section 105: The Superficial Safeguard of Videography

One of the notable features of the BNSS is Section 105, which makes audio-visual recording of search and seizure mandatory[29]. While Section 105 of the BNSS is intended to prevent police misconduct in search and seizure operations and the planting of evidence, its focus is entirely hardware-based[30].

Without recording what specific folders were opened, what files were copied, or what keywords were searched at the scene, videography remains a superficial safeguard.[31] It provides a false sense of security while doing nothing to prevent "digital over-reach" or the violation of irrelevant personal data.[32]

V. Jurisprudential Gridlock: Competing High Court Paradigms in Criminal Justice

In the absence of express statutory guidance in the BNSS, the Indian Judiciary appears to be divided between two competing models of criminal justice.

A. The Crime Control Model: Virendra Khanna v. State of Karnataka

In Virendra Khanna v. State of Karnataka, the Karnataka High Court was of the view that the state's interest in efficient investigation should take precedence over the right to privacy[33]. The

---

[27] *See* Katz v. United States, 389 U.S. 347 (1967).

[28] *See* SC Observer, *Constitutional principles go for a toss in the criminal law of search and seizure of digital devices*, https://www.scobserver.in (last visited Jan. 28, 2026).

[29]BNSS, sec 105.

.

[33] Virendra Khanna, 2021 SCC OnLine Kar 5032.

Karnataka High Court held that the act of furnishing a password was not 'testimonial' in nature because it was not a 'statement of fact' in relation to the commission of the crime. The act of furnishing a password was a physical act analogous to furnishing a key to a physical locker[34]. The Karnataka High Court was of the view that an adverse inference might even be drawn against the accused for his failure to assist in the decryption of the evidence[35]. The 'Crime Control' model appears to have been adopted in the Virendra Khanna case, wherein the efficiency of the criminal investigation process has been allowed to take precedence over the rights of the accused. The smartphone has been treated as nothing more than a 'container' of evidence[36].

B. The Due Process Model: CBI v. Mahesh Kumar Sharma

In a stark contrast to the Virendra Khanna judgment, the Special CBI Court in Delhi, with observations from the Delhi High Court, held in the case of CBI v. Mahesh Kumar Sharma that the accused cannot be compelled to disclose the passcode of his smartphone[37]. The Special CBI Court was of the view that the act of furnishing a password was a 'volitional act of memory,' which was protected under the doctrine of 'mental privacy' under the Selvi judgment[38]. The 'Due Process' model appears to have been adopted in the CBI v. Mahesh Kumar Sharma case, wherein the smartphone has been treated as a 'repository of thoughts.' The Delhi High Court was of the view that the state must access the evidence in the smartphone through its forensic capabilities rather than through the mental compulsion of the accused[39]. The divergence in the views of the Karnataka High Court and the Delhi High Court has resulted in a geographical disparity in the rights of the accused, depending upon the jurisdiction of the High Court.

---

[34] Id at para 45

[35] Id

[36] *See* Herbert L. Packer, *The Limits of the Criminal Sanction* (1968) (defining the Crime Control vs. Due Process models).

[37] CBI v. Mahesh Kumar Sharma, Special Case No. 20/2022 (Special CBI Court, Delhi).

[38] Id.

[39] Id.

C. The Media Professionals Case: A Potential Alternative Path?

It was recently recognized by the Supreme Court in the case of Foundation for Media Professionals v. Union of India that the unique risks to journalists whose electronic devices are seized may be recognized by the Court[40]. The Court recognized the risk of the free power of search resulting in the divulgence of sources and the chilling effect on the freedom of the press as guaranteed by Article 19(1)(a) of the Constitution.[41] It may be argued that the Special Guidelines may be applicable to all individuals as a matter of the Right to Privacy[42].

VI. Technological Imperatives: The Forensics of Selective Extraction

At the heart of the so-called "digital strip search" is the technological tendency to over-collect data. The mobile forensic tools used by Indian investigators (such as Cellebrite's UFED, MSAB's XRY, and Magnet Forensics) have varying capabilities in terms of data extraction[43]:

A .Hierarchy of Extraction

1. Logical Extraction: The least invasive, maintaining the highest level of privacy by only allowing the extraction of data currently visible to the user, without access to deleted data or system files.
2. File System Extraction: The more invasive version, allowing the copying of the internal database files, as well as the extraction of hidden data and application caches.
3. Physical Extraction (Bit-by-Bit Imaging): The most invasive, allowing the creation of an exact replica of the flash memory, including unallocated space, and thus the possibility of deleted files.

---

[40] Foundation for Media Professionals v. Union of India, W.P. (Crl.) No. 495/2022 (Supreme Court of India).

[41] Id.

[42] Id.

[43] *See* Cellebrite, *Cellebrite UFED: The Standard for Digital Intelligence*, https://www.cellebrite.com (last visited Jan. 28, 2026).

B. Forensic Sledgehammer versus Scalpel

Indian investigators have consistently used the Physical Extraction method due to its increased potential to recover evidence.[44]However, this is precisely the equivalent of the "forensic sledgehammer." Advanced forensic tools have the capacity to limit the extraction of data according to specific parameters:

- Temporal Filtering: Data is restricted to a specified time period.
- App Filtering: Data is restricted to WhatsApp, excluding Health or Financial Apps.
- Category Filtering: Data is restricted to Images, excluding Text Messages.[45]

The failure to mandate the process of selective extraction by the BNSS results in the sledgehammer remaining the norm. The failure to recognize the technical possibility of the 'forensic scalpel' results in the State violating the 'Necessity' test, as prescribed by the Puttaswamy test.

C. The Significance of Hashing & Chain of Custody

The legal validity of digital evidence is predicated on the 'Hash Value,' which is the unique 'digital fingerprint' of the data, e.g., MD5 or SHA-256 hash value[46]. If the device is seized without the corresponding 'Hash Value' being given to the accused at the time of seizure, it cannot be guaranteed that evidence is not 'planted' on the device.[47] This issue was at the heart of the Bhima Koregaon controversy, where it was asserted by international forensic experts that the possibility of the use of 'malware' to introduce evidence on the accused individuals' devices could not be ruled out. Notwithstanding the above, the BNSS fails to mandate the 'Hash Value Handover' procedure.

---

[44] Id at 10

[45] MSAB, *MSAB XRY: Mobile Forensic Extraction*, https://www.msab.com (last visited Jan. 28, 2026).

[46] CENT. BUREAU OF INVESTIGATION, CRIME MANUAL 2020, Ch. 14 (Govt. of India 2020).

[47] SentinelOne, *Modified Files Found in Bhima Koregaon Case*, https://www.sentinelone.com (last visited Jan. 28, 2026).

VII. Victimology and Secondary Victimization

An underlying principle of the current reform is that the BNSS places significant emphasis on the victimology approach. However, in the digital world, legal procedures often facilitate secondary victimization.

A. The Voyeuristic Investigation

In sexual offense cases, technology-assisted abuse, and stalking cases, the practice of performing a "digital strip search" of the victim's phone is ubiquitous in the digital world.[48] The defense and investigators scrutinize the entire life of the victim, from past relationships and photos to personal communications, in order to obtain information that could potentially discredit the victim's testimony.[49] This is the digital equivalent of the prohibited "bad character" evidence in physical cases.[50]

B. The Trauma of Data Loss

To many victims, their smartphone is their sole means of protection, communication, and proof of their abuse. The confiscation of their phones for extended periods of time without providing a backup copy results in digital isolation and re-traumatization for victims. A truly victim-centric approach necessitates the creation of a "Mirror Image" and the prompt return of the physical device to the victims, which is not guaranteed in the BNSS system.

VIII. Professional Privilege and the Erosion of Confidentiality

The indiscriminate seizure facilitated by Sections 94 and 185 of the BNSS threatens Privileged Communications protected under the Indian Evidence Act (now BSA).[51]

---

[48] *See* POCSO Act, 2012, No. 32, Acts of Parliament, 2012 (India).

[49] Id.

[50] *See* Indian Evidence Act, 1872, sec 53A (prohibiting character evidence in sexual offense trials).

[51] Bharatiya Sakshya Adhiniyam, 2023, No. 47, Acts of Parliament, 2023 [hereinafter BSA].

A. The Lawyer-Client Privilege

By seizing a lawyer's phone, the State acquires privileged documents belonging to all his or her clients, not just the targeted individual[52]. This compromises Legal Professional Privilege (LPP), which is a fundamental component of the Right to a Fair Trial under Article 21 of the Indian Constitution[53]. There are no provisions for "filter teams" or "taint teams" in the BNSS that would restrict investigators from accessing privileged communications.

B. Medical Privilege and Spousal Privilege

An analogous risk exists in medical confidentiality and spousal communication[54]. A digital search would not distinguish between an incriminating communication and a privileged communication. The absence of provisions for Privilege Filtering in the BNSS is a critical legislative oversight that may be challenged on constitutional grounds.

IX. Comparative Jurisprudence: Global Benchmarks

India's regime is also distinguishable when viewed in the context of the regulatory evolution in other major democracies, which have sought to update their legislative regimes to address the digital age considerations.

A. The United States – Riley v. California

The United States Supreme Court, in the case of Riley v. California, unanimously ruled that the Search Incident to Arrest warrantless search exception does not extend to searches of the contents of cell phones[55]. According to the majority decision, "Cell phones differ in another, important respect. Unlike the physical items in the majority's hypothetical, cell phones are not just another technological convenience. With all the information, data, and records that they store, cell phones have become information repositories of immense private importance. The privacies of life are

[52] *In Re:* Summoning Advocates and Seizing Devices, 2025 SCC OnLine SC 112 (India).

[53] Id.

[54] *See* BSA, sec 132, 128 (protecting privileged communications).

[55] Riley v. California, 573 U.S. 373 (2014).

those personal to the individual, such as the contents of one's home, correspondence, and conversations." [56]Therefore, the Court held that, absent an emergency, the government must obtain a warrant prior to the search of the contents of a mobile phone[57].

B. The United Kingdom – The Police, Crime, Sentencing, and Courts Act 2022

The United Kingdom's Police, Crime, Sentencing, and Courts Act 2022 includes the imposition of a separate Code of Practice relating to the extraction of digital data[58]. The regime requires the extraction to be "strictly necessary" to the proposed line of inquiry, the preference being for selective data extraction where possible. Additionally, the regime requires the investigator to provide the data subject with a Privacy Notice clearly outlining the data to be extracted[59].

C. The European Perspective – The Right to be Forgotten and Seizure

The European perspective on the issue is reflected in the Erasure or the Right to be Forgotten, which requires the state to erase all digital data generated during the investigation, upon the conclusion of the investigation. Unlike the BNSS regime, the framework does not require the state to erase the data, thereby allowing the state to maintain permanent digital records of the individuals who were the subject of the searches.

X.Conclusion and Policy Recommendations: Towards a Digital Evidence Code

The shift from the Code of Criminal Procedure (CrPC) to the BNSS is marked by an apparent legislative paradox: the application of modern tools to fortify an outdated 19th-century model of complete state control.80 To ensure that the procedural adoption of modern tools does not undermine individual privacy, the following systemic reforms are suggested:

Enactment of Digital Evidence Code: The Central Government is recommended to enact rules under the BNSS that draw a distinction between hardware seizure and data collection, with an emphasis on the collection of relevant data instead of hardware seizure.

---

[56] *Id.* at 393.

[57] Id.

[58] Police, Crime, Sentencing and Courts Act 2022, c. 32 (UK) [hereinafter PCSC Act].

[59] Id.

2 Mandatory Judicial Warrants for Digital Searches: The existing exception of "undue delay" in Section 185 of the Act is recommended to be closed by making it mandatory to obtain a judicial warrant before any digital search is executed, specifying the application, files, and timeframe to be searched.

3 Hash Value Handover: It is suggested that it must be made a statutory requirement to generate and convey a hash value to the device owner at the site of search to prevent any act of tampering
.

4. Codification of Selective Extraction: Forensic services should be prohibited from engaging in physical imaging unless they can show a court that it is not feasible.

5. Establishment of Separate Taint Teams: In order to protect professional privilege, a separate body (or a judicial officer) should review extracted material before it is provided to the investigating officer.

6. Right to Mirror Imaging: In the case of victims and witnesses, legislation should ensure that their devices are returned within 24 hours following the taking of a mirror image to prevent digital dislocation.

The Digital Strip Search is a key issue facing civil liberties in our era8. As the BNSS makes its way through the Indian judicial system, it is essential that the judiciary fill the constitutional gaps left by the legislature. If justice is not both tech-savvy and constitutional in scope, then there is a danger that India will become a digital panopticon in which Indians are denied their dignity