Partners Universal International Research Journal (PUIRJ)
Volume: 04 Issue: 04 | October– December 2025 | ISSN: 2583-5602 | www.puirj.com

Sanchar Saathi Digital Security versus Civil Liberty in India 's Smartphone Era

Dr.A.Shaji George

Independent Researcher, Chennai, Tamil Nadu, India.

Abstract - In December 2024, India briefly issued a directive, obliging all smartphones to pre-install the Sanchar Saathi cybersecurity app. The mandate was abandoned within 24 hours under strong popular criticism and industry pressure. The rapid turnaround demonstrates democracies reaction to the issues in technology policy and the effect of social responsibility. The population of mobile users in India is 1.2 mobile users but only 37% digitally literate. Another problem that the country has to deal with is the issues of huge underground markets of stolen phones with false IMEI numbers and advanced digital fraud. The first option was a state-operated application that demanded a large percentage of device rights. This posed some serious concerns regarding constitutional privacy, openness in technology, and the way in which democratic institutions manage such requests. The justification used by the government to justify the turnaround was 600,000 voluntary registrations in a day, 10 times the amount. Although it is democratic responsive, it does not address the fundamental cybersecurity lapses. The article considers technical architecture, international precedents and constitutional structures by analyzing this policy episode. It holds that there is a false dichotomy between security and privacy. The article provides alternatives that can be put into practice to protect citizens without interfering with civil liberties, which are listed using examples of Singapore, EU, and other jurisdictions. It provides some handy resources that can be used by legislators, technology companies, civil society, and individuals to demand privacy-friendly security systems. Although the controversy was settled within a short period of time, it was a major landmark not only in India, but also in the way developing democracies in the world influence the digital sovereignty in the face of increasing technological governance pressures.

Keywords: Digital surveillance, Privacy rights, Cybersecurity governance, Mandatory app installation, Democratic accountability, Data protection, Civil liberties, Technological authoritarianism.

1. INTRODUCTION

1.1 Protection Becomes Intrusion and Citizens Push Back

India In December 2024, the 1.2 billion mobile users in India were informed that the government had a new policy only to renegotiate it in 24 hours. The Ministry of Electronics and Information Technology had given a directive that all new phones sold in India need a pre-loaded application named Sanchar Saathi (communication companion). It was a bold strategy all the new devices would have the app installed within 90 days, and the updates will be imposed on the phones already in possession. The said objective was to save individuals against online fraud, stolen phones with falsified IMEI numbers and other cybercrimes. However, the roll out of the plan immediately met with vehement opposition, and the government was forced to change the policy to the point of opposition.

The App poses issues which go way beyond India:

- When does fair security become an intrusion into surveillance.

- In a system where a government purports to be the defender, how can the citizens be assured of the real functionality of the app.
- What happens when the masses are opposed to a compulsory state application on their individual gadgets.

Sanchar Saathi is referred to as a cybersecurity call center and complaint center. Formally, the app is supposed to assist in case you purchase a phone with a counterfeit IMEI, a stolen phone or if you have become a victim of a SIM swap. It was marketed by the government as a digital emergency service, which appeared to be a reasonable idea based on the fact that India is facing an increasing digital fraud crisis.

But there were pre-installation sob-sisters on all sides of the political gamut. The opposition leaders termed it as a surveillance machine. Privacy activists cautioned that an app with complete access to devices may in theory monitor every move by the user. Civil liberty organizations claimed that it infringed the basic right to privacy as stated by the Indian Supreme Court in 2017. The technology analysts were puzzled as to why a reporting tool needed such a wide permission. Even the world producers such as Apple were seen to have come out refusing to comply as they resisted the mandate.

The 24 -Hour Reversal What Changed

The government overturned the requirement in a day of the backlash. According to the press release of the Ministry, it is in light of the growing acceptance of Sanchar Saathi that the government has resolved to avoid pre-installation of mobile manufacturers. It was justified by the fact that there were 600,000 new registrations in one day that was a tenfold increase, which proving that voluntary adoption made mandatory installation unnecessary.

Such a number constitutes less than 0.05% of the population of India that enrolled when the announcement was made. The surge was described by the critics as superficial and politically motivated because many users merely tested what the app actually did and did not, in fact, adopt it. There was skepticism in public opinion it can make the old boomers believe these figures everybody knows what they are attempting to do- it is merely a means of keeping track of what people are doing.

The inversion brought into focus a number of dynamics:

1. Public resistance works. Not silent obedience but vocalized protest by the citizenry, both technologically minded young people and privacy minded adults, through social media, commentary in the press, and on the street.
2. The resistance in the industry is important. Large producers, in particular, Apple, did not want to comply, and the government had to face economic and reputation expenses.
3. The government provided a way-out excuse. Instead of acknowledging overreach, the officials framed the reversal as something unneeded because of voluntary achievement, which was a political recession that avoided admitting error.
4. The issues that lie behind are not addressed. Cybersecurity issues that inspired the mandate fake IMEI devices, advanced fraud schemes, inadequate consumer protection, etc. remain unaddressed holistically.

1.2 The Real Security Challenge That Survives

Nonetheless, the policy reversal notwithstanding, India has a huge digital security crisis that must be addressed. The market of second hand phones is large and unregulated. Devices that are stolen and

blacklisted are resold freely and purchasers have no substantial mechanisms of assuring themselves. The phones with cloned or counterfeit IMEI numbers are available freely and cause severe vulnerabilities.

The repercussions go beyond loss of money. In the worst-case scenarios, the innocent buyers are associated with crimes committed by using the devices that they buy. Think of purchasing what you suppose is a rightful second-hand phone, and later being caught by the law enforcement tracing illegal proceedings to its IMEI number which is currently in your hand. Consumers are not shielded unless it is verified strongly. The unregulated market was of genuine concern to the government. The solution that was selected was not mandatory state app installation with extensive permissions. It is important to be aware of actual security threats but not to embrace invasive measures that undermine privacy and autonomy.

1.3 The Surveillance vs. Security Controversy

The Sanchar Saathi scandal revealed some of the underlying conflicts of digital governance. The officials said that the app was optional, could be removed, did not collect any personal data and only helped to report. But the installation requirement was a mandatory directive that went against these assurances. In case it is optional indeed, why should it be pre-installed on all the devices. In the event that it gathers no information, why give it massive privileges.

The permissions of the app were much more than the functions it was supposed to have, as critics remarked. These included:

- Telephone call capability and management.
- Send and access messages
- Call log in and out
- View message history
- Browse pictures and files on the device memory.
- Use the phone's camera
- Have a cost of being on at all times.

These permissions are warning signs to a simple reporting tool. To report a stolen phone, location tracking is not required. Scam alerts do not require access through SMS. IMEI is not checked in call log access. The background operation allows the user to be constantly monitored even when the application is not being actively used.

The technical fact is harsh competence has more to play in security analysis than goodwill. The implementation of an app with surveillance features may now be used only in legitimate ways, whereas the features are also present. The infrastructure can be reused by future governments or a shift of priorities or missions without needing additional technical development.

1.4 International Context and Democratic Stakes

The Sanchar Saathi controversy is not a single incidence but a general world trend where governments are trying to have a closer regulation of digital infrastructure.

China has established a large surveillance system that compels people to install compulsory apps. These applications monitor movements, products and communication and the state operates a social credit and facial-recognition system.

Russia also requires telecommunication companies to install equipment that will provide intelligence services with direct access to all communications. The nation also requires state applications and restrains VPN.

On the contrary, the European Union lays stress on privacy. Its GDPR incorporates the harsh penalties on misusing data and insists on openness, placing the individuals in authority.

The majority of democracies are in the middle between those extremes. When there are no clear guidelines on security and privacy, they find it difficult to balance both. The United States has been engaging in a lot of surveillance through some of their agencies, however, a certain level of domestic monitoring is restricted by the constitution. The demand of backdoors by the law-enforcement is controversial in Australia. The United Kingdom is very vigilant in communication spying but the courts would not hesitate to question any privacy infringement.

The quick change of mind of the Sanchar Saathi requirement in India shows that democracy does not fail in accountability. Even great democracies need to think when its citizens raise their voices and manufacturers strike back. This leaves a precedent elsewhere in the developing democracies, civic resistance against surveillance may be effective.

1.5 Article Objectives and Structure

This article analyses the case of Sanchar Saathi controversy the original mandate of the program to reverse within a short period of time to provide some lessons on democratic digital governance.

Objectives:

- Personally engage in reporting a balanced and full analysis that does not resort to partisan rhetoric but considers the technical, legal and social consequences.
- Inform readers about the contemporary global issues of digital governance, and place Indian experience in the context of the global patterns of growing state intervention in the digital infrastructure.
- Seal major gaps concerning the reality of what Sanchar Saathi does, what it seeks to have, how its structure looks in comparison with other international systems and what the legal protection is or ought to be.
- Provide viable models to stakeholders policymakers require security models that consider civil liberties the technology companies require balancing between compliance and ethics the civil society requires the advocacy tools and the citizens need to be provided with actionable privacy measures.
- Demonstrate that, though it is positive, the reversal does not resolve all the issues. India requires strong cybersecurity that will safeguard the consumers against fraud and stolen devices without undermining the constitutional privacy rights.

The stakes are high. The decisions made by India change the relationship of 1.2 billion people with technology and can serve as an example, which other nations can either emulate or disapprove of. Whether India will lead by example and be a democratic example of digital governance or a cautionary note of the dangers of excessive security will depend on whether it chooses a model of surveillance-heavy security or increased privacy.

1.6 Research Methodology and Limitations

Data Sources:

- Government announcements, Government notifications, and press releases on Sanchar Saathi. The statement of reversal and justifications.
- Social-media feedback and other public commentary indicating the concerns of the citizenry.
- Technical documentations of the Sanchar Saathi platform (where possible).

Overall, the comparative study of global digital-governance structures.

The constitutional law in India, particularly the 2017 Puttaswamy judgment on privacy.

- Published cybersecurity statistics provided by the government and in independent sources.
- Smartphone company reactions in the industry.
- News stories and the punditric commentary.

Limitations:

Technical gaps Technically, the full source code and detailed specifications are not publicly available, which makes it difficult to check the capabilities.

- Fast transformation - the turnaround took less than 24 hours the details of the implementation, rationale and the long-term consequences are not yet developed.
- Lack of transparency- government has not published complete privacy policies, technical architecture, data-handling process, or independent audit findings on Sanchar Saathi.
- Registration uncertainty 600,000 registrations claimed in a single day cannot be authenticated as such and no one knows whether these are voluntary or investigative.

Research Approach:

The article conducts the evaluation of the balance between the legitimacy of security objectives and privacy protection by applying comparative policy analysis, assessment of constitutional law, and assessment of technical architecture (through the available information) and risk assessment (through the use of international precedents).

The paragraphs below discuss the state of digital vulnerability in India, the global trends, a stepwise analysis of the operations and authorization related to Sanchar Saathi, the dynamics of the reversed mandate, the constitutional and technical privacy arguments, the implications of the reversal on democratic accountability, and practical recommendations on the construction of privacy-protecting security infrastructure.

2. OBJECTIVES

2.1 Understanding the Stakes

We should first define what this article is intended to accomplish and why before we go deep into the details. We intend to provide a balanced, broad analysis of Sanchar saathi controversy. We would rather get beyond partisan rhetoric and examine the actual technical, legal and social consequences. It is too frequent that the debate on technology and privacy divides into two camps the camp of security and the camp of privacy, the

camp of trust and the camp of mistrust of government. The reality is more nuanced. Security and privacy are two real issues that should be taken seriously. It is not a task to decide between the two, but to create systems that safeguard the two.

Second, this article is an attempt to inform the readers on the subject of digital governance in democratic societies. The Sanchar saathi was a requirement that emerged in the wider international tendencies. The role of states in digital infrastructure is growing, cybersecurity issues are becoming more and more significant, and without appropriate structures, democracies can barely control technology. The awareness of these trends explains why this controversy is important and what precedents it might have.

Third, we would like to fill in the key information voids. A lot of the Sanchar saathi debate principally occurs in the absence of facts. What does the app do. What are the permissions it seeks. What is the comparison of its architecture with other global apps of the same kind. What are the legal protective measures against abuse. In the absence of answers, discussion is not informed but rather speculative.

Fourth, this paper provides practical guidelines to different stakeholders. Policymakers require models that attain legitimate objectives and do not violate civil liberties. Technology companies should be advised on how to strike balance between compliance and ethical accountability. The civil society organizations require advocacy tools. People require effective actions to defend privacy, and become democratic. Generalized advice is of no use we require concrete and practical action plans.

Lastly, this article hopes to serve as an inspiring moment, not one of giving up. One would find it simple to believe that citizens cannot rebel against government orders or that there is no privacy in the cyber world. Neither is true. Democracies evolve as citizens require it and technology is the development of the values we inculcate. The Sanchar saathi controversy is a chance to build improved digital governance, however, only when the sufficient number of individuals is aware of the stakes and courses of action.

These aims can be important since there are real and high stakes. The current choices of digital infrastructure made by India will impact the future relationship of 1.2 billion people with technology. They will make India a surveillance state or a democracy that respects privacy. They will provide precedents that will be imitated or denounced by other countries. And they are going to determine whether ordinary citizens will continue to have meaningful control over their digital lives or be passive subjects of technology control.

3. THE DIGITAL VULNERABILITY LANDSCAPE

3.1 Understanding India's Mobile Security Crisis

In order to understand the rationale behind why the government believes Sanchar saathi is necessary we must face an ugly reality, which is that India is experiencing a massive, growing, and relatively unmitigated digital security crisis.

The figures are a terrible tale. India has approximately 1.2 billion mobile-phone users, which is the second-largest mobile market in the world following China. This incredible digital penetration is commendable as a developing nation. The smartphone is now the primary means by which individuals can access the internet, conduct banking, communicate with loved ones, government services and also be involved in the economy. To hundreds of millions of Indians, their phone has become a bank, their office, a library and a lifeline.

But here is the problem. There are 1.2 billion mobile phone owners in the world whereas only 37 percent of the Indians are digital literate. Almost two out of every three users do not have the fundamentals to use the web

safely. They are not able to notice phishing, evaluate app-request permissions, determine the authenticity of websites, and evaluate the dangers of digital security. It is this gigantic weakness, which criminal minds are taking advantage of.

The magnitude of online fraud is astronomical. Through a one-time government crackdown, the government disconnected 11 million mobile connections associated with fraud. Consider that figure somewhere about the people of Belgium. These were not some of the suspicious accounts these were registered fraud, scam or illegal activities users.

It was also during this operation that about 50,000 fake or stolen handsets were discovered. They resemble actual phones but have malware, spyware or backdoors that allow criminals to have full access to the information of the user. They are being sold at high prices in the underground markets, where price sensitive consumers, who are unable to authenticate, cannot resist.

Governments also blocked 1.1 million fake WhatsApp accounts. They were applied to scams of various kinds such as impersonating the government bodies that required money to romance scams that robbed life savings. Today hackers are able to copy voices and use artificial video calls and create realistic documents with the help of AI. Common people do not have a defense mechanism against such tricks.

They also blocked 71,000 SIM sellers that were involved in fraudulent activities through the creation of documents. These sellers enrolled SIMs under stolen identities or counterfeit credentials and used them to commit all kinds of crime such as financial fraud as well as terrorism. The true users could not be traced in any way.

The human cost is exhibited in real life. Consider the most widespread and most devastating scam SIM-swap. The criminal collects personal details which are not very difficult to locate such as your name, phone number and address. Then they go to a mobile provider and state that they had lost their SIM and that they are you. In the event that the provider does not check the issue, they re-issue another SIM with your number. The criminal gets all your calls and texts including one time passwords of your bank accounts in a flash. They are able to empty your pockets in a few hours. The victims find out about the fraud at the wrong time.

Consider fake banking apps. The criminals develop applications that resemble genuine banking applications, including stolen logos and interfaces. They advertise them in search results or social media advertisements or even app stores in case they get through review procedures. Little unsuspecting users download the applications that they believe to be the official app of their bank and provide their credentials. Their accounts are now at the mercy of the criminals.

Phishing attacks have become extremely advanced. A text may seem to be sent by a governmental service, including an official sender ID and formatting. The message says that there is an issue with your tax filing, Aadhaar card or COVID vaccination certificate and there is a link to check your status. The connection takes you to a persuasive counterfeit site in which you are requested to provide confidential details. When you do, you risk being robbed by criminals or hackers into your accounts.

The monetary expense is immense. The detailed information is difficult to obtain since most of the victims do not report the fraud, either because of embarrassment or due to the fact that nothing can be done. It has been estimated that Indians are losing billions of rupees a year to online scams. According to the reserve bank of India, in the year 2023 alone, there was an increase of 28% in the banking frauds. Frauds involving credit-cards, identity theft and web scams are on the rise each year.

What is the reason why conventional methods have not been effective in holding this crisis. Several factors contribute.

To begin with, there is fragmentation in the enforcement. There are several jurisdictions of cybercrime. Police in the local areas are not usually trained or equipped to probe digital fraud. The responsibilities of the state and central agencies are similar and there exists poor coordination. Before any complaint is processed by the bureaucracy, it is too late, criminals are gone.

Second, there is a low level of awareness to the users. Cybersecurity awareness campaign by the government is present but it has a very small proportion of the population. The majority of individuals get informed about digital security when they fall victims. They do not have a systematic education about how to be aware of scams, how to protect their personal information or how to use devices safely.

Third, the absence of regulations allows the criminals to perform impunity. India does not have any detailed data-protection laws. Companies which do not secure user data have no meaningful penalties. Cybercrime faces a weak enforcement mechanism and limited international collaboration on cybercrime, thus criminals have the opportunity of acting within jurisdictions that are not within the jurisdiction of the Indian law enforcing the criminal law.

Fourthly, the black market is large and advanced. Criminal networks purchase and market stolen information, forged documents, stolen accounts and hacks. These networks are open on some social networks secured by encryption and anonymity. Disabling a single operation is of very little use when ten more pop up.

Sanchar saathi is based upon this argument by the government. According to the officials, classic methods, such as public awareness campaigns, better enforcement of the law, and better coordination, are not enough. According to them, direct intervention with the help of technology is required. When a citizen won't download security software on their own, when they will be not able to detect fraud without any assistance, and when the current system is unable to safeguard them, maybe the answer is to pre-install security software to their computers. This argument has merit. India really requires to have superior digital protection infrastructure. Millions of vulnerable users are failing due to the status quo. Something has to change. The issue is, however, should a government app be required to be installed, or are there alternatives to the issue that are less intrusive and yet, will guarantee the same level of security. That is what we have to investigate further.

4. CURRENT TRENDS

4.1 The Global Shift Toward Digital Governance

The Sanchar saathi requirement is placed in a wider international framework of the governments taking control over the digital infrastructure. These trends can be used to explain what is at stake in India.

The question of the way to control digital space is being negotiated across the world as democracies and autocracies find ways of governing them. The initial incarnation of the internet was founded on openness, decentralization and limited regulation. That era is decisively over. The governments have come to regard digital infrastructure as national security similar to physical roads and abandoning it to companies is simply unacceptable.

The directions taken by the various countries differ radically. China has constructed the most comprehensive system of digital surveillance in the world. Great Firewall is a censor of what the citizens can read. Compulsory applications monitor movements, transactions, and communications. A social-credit system is a reward

system that rewards conformity and punishes deviance. Facial-recognition cameras monitor the open areas. This is digital dictatorship in all its manifestations.

Russia adheres to the same direction, albeit at a lesser level of comprehensiveness. The SORM system compels the telecommunication providers to install equipment that would avail all the communications directly to intelligence agencies. There are compulsory apps that track COVID, finance, and others. VPNs are blocked. Experiencing pressure to conform or to leave, foreign internet firms are compelled to acquiesce or resign.

The other extreme, namely the European Union, values the protection of privacy. The General Data Protection Regulation provides people with unprecedented access to personal data. It subjects severe fines to the organizations that abuse information and brings transparency. EU is of the notion that privacy and security can co-exist provided they are well controlled.

The majority of democracies are in between these two extremes, and attempting to strike a balance between security and privacy, without explicit guidelines. The U.S. has strong spying abilities by certain bodies such as the NSA, but domestic spying is restricted by the constitution. Australia demands the development of law-enforcement backdoors by tech companies but it is debatable whether this would undermine the security of everybody. U.K. has a high level of monitoring of the communications in order to keep the country secure but is always challenged in court over the violation of privacy.

There are a number of trends that crop up in this landscape. To begin with, technological organizations are pressured more by the governments to join in state secrecy. Companies, whether by law, or informal pressure, are supposed to provide user data, create access control, or delete content that governments consider problematic. The distinction between collaboration and force has faded.

Second, there are more mandatory applications. COVID contact-tracing apps familiarized a lot of individuals with software enforced by government on personal computers. Although this was said to be voluntary, social pressure, employment conditions or even restrictions to access meant that most people had few options. This has been a precedent that is being applied to other uses by governments.

Third, voluntary downloads are substituted by pre-installation as a more desirable form of distribution. Many governments discover that good intentioned applications fail to get to users unless they have to install them. Apps that are pre-installed assure saturation. All the devices become a possible surveillance or security endpoint, depending on the functionality of the app.

Fourth, the transparency is declining as opposed to rising. The governments install security or surveillance systems without recording abilities, lack of auditing and without any serious monitoring. They provide guarantees, yet verification is rejected. This trust us model goes against democratic accountability.

Fifth, all these trends were boosted by the COVID pandemic. They were passed by governments that could have been debating the issue of surveillance years and justifying them by the emergencies of a pandemic. The infrastructure is built rarely and once it is built, it is hardly removed. Emergency powers are rendered permanent. Applications developed to monitor health are used to monitor other things.

India is an apt fit in such global trends. The Aarogya Setu contact-tracing application established the precedents of mandatory government applications. Although it was being sold as voluntary, it was necessary when travelling by air, when entering an office and many others. It was downloaded not voluntarily but as a necessity by millions of individuals. The app was gathering information on location, Bluetooth proximity and

health data. The advocates of privacy expressed their concerns regarding the security and misuse of the data. The government provided guarantees but did not go into technical documentation.

Now, Sanchar Saathi, the government is also making the next step. It will exceed obligatory of particular activities. It is going to be installed in each device. It will not be momentary but permanent. It will focus on a wide objective of cybersecurity, which may encompass almost anything.

The knowledge of these trends explains why the Sanchar saathi controversy is of international interest. India has moves that are observed by every democracy. When the largest democracy in the world could impose the pre-installed applications of the government without stringent privacy safeguards it will be creating a precedence that can be emulated by other emerging democracies. It naturalizes a digital form of governance that puts the state in first place, as opposed to individual autonomy.

On the other hand, when India develops an improved version, one that can deliver a reasonable security not violating the privacy and at the same time in a democratic accountability, then it would provide an alternative model that other countries experiencing the same strains can emulate. India will send shockwaves to the world with the decisions it takes regarding Sanchar Satyam.

5. DECONSTRUCTING SANCHAR SAATHI

5.1 What the App Actually Does

To shed the speculation we have to examine in detail what Sanchar saathi is and what it purports to be. Openness is a critical issue in this case. The majority of information has been provided out through government utterances and scanty technical documents rather than direct verification.

The official descriptions state that Sanchar saathi is a cybersecurity application, which shields mobile users against fraud, theft, and hacking. The application boasts of a number of functions.

First, it is used as a reporting center. Users may make complaints on stolen phones, fake phone models or internet fraud. The application allows them to explain what occurred, and provide details and hand in the complaint to the authorities. It will ease this process, and it is not as difficult as it is in the traditional police reporting.

Second, it has device verification in the app. The users can also verify the authenticity of their phone, and confirm the theft. It can communicate with government IMEI databases to establish the device status and also prevent the sale of stolen and fake handsets.

Third, it gives cybersecurity notifications. The application alerts its users on recent scam patterns, novel modes of fraud, and other threats. The concept is to teach the users on the spot, when they are most likely to pay attention to it, instead of abstract awareness campaigns, which can be disregarded.

Fourth, Sanchar has in-built reporting of suspicious calls, texts, or app actions. In case you believe that you are phished, the app allows you to report it. Should an unidentified person request you to provide some personal details, you can mark it. The consolidated information is reportedly useful in enabling the authorities to track and close fraud activities.

These functions are reasonable and useful. An efficient reporting system may be used to enhance the current procedures. Verification of the device would save the consumers of purchasing stolen or counterfeit phones. Live warning systems would possibly stop fraud. Convenient reporting may assist the authorities to respond more quickly to new threats.

The issue lies in the difference between the functions stated and the real abilities. The purpose stated by an app may not be what it can do. Request of permission is critical. Provided that Sanchar saathi would just fulfill the functions listed above, it would require the minimum number of permissions it must have internet access to submit the reports, perhaps camera access to scan device data, and perhaps even contacts access to report suspicious numbers in the call log.

Nonetheless, the information that is accessible indicates that the app demands much greater permissions. Precise information is not evident (that is why transparency is important). The standard Indian government apps will demand access to location, SMS, access to call logs, storage access, and background executable applications even when idle. All these permissions offer functionality that goes way beyond the mentioned functions.

Location tracking, such as, does not require one to file a complaint or inquire whether your phone is stolen. But it would allow the app to keep track of your movements, creating an extensive map. There is no requirement to use SMS to send warnings on trending scams, although it would enable the app to access all messages, including single passwords and conversations. The access to call logs might expose your communication activities including whom you converse with, frequency, and duration of the call. Access to storage could provide access to photos, documents, and other files. Of particular concern is the option to operate in the background. The constantly running apps can keep track of you even when you are not even conscious of it. They are also able to monitor the apps that you utilize, the websites that you pay attention to, the things that you type, among others. This makes one security app more of a surveillance tool.

The officials of the government claim that these worries are exaggerated. They assert that Sanchar is not tracking them with these permissions and that they are only allowed to track the legal purposes of the app and that there are strong defenses against abuse. However, until there are independent technical inspections, open source code and transparent legal boundaries to data collection and usage, such guarantees are empty.

The fact that India is not transparent can be seen by comparing other global applications. The Scam Shield app of Singapore is open source. Independent researchers are able to review the code, check the level of data it gathers, and ensure that it does not do anything it purports to do. The privacy policy of the app provides a clear understanding on what data is being gathered, how it is being used, and how long it will be held as well as by whom. Compliance is checked by regular third party audits. The users will be able to view what they are actually consenting to.

The UAE eCrime platform operates in a different manner, where it primarily operates as a web service instead of an obligatory application. The end-user can report cybercrimes through a website or voluntary application, but he or she does not need to install anything on his / her personal machine. This will accomplish this by having a streamlined reporting without the consideration of privacy issues in the form of pre-established surveillance functionalities.

South Korea has a balance of security and privacy, as there are stringent data protection laws that apply to both government applications. These applications should be evaluated by privacy impact assessment prior to their implementation, reduce data gathering to the bare minimum, seek direct consent to sensitive permissions, and be controlled by external audit and sanctions on breach.

The practice by India towards Sanchar Satyam has no such safeguards. The app is not open source. Its capabilities have not been verified by any independent audit. Privacy policy which is elaborated upon has not

been extensively popularized. The manual permissions requested are unknown to many of the users. There is no legal framework to regulate data collection, retention, and access or it is not sufficient.

Here lies a very important difference. It is not whether Sanchar Satyam now practices mass surveillance--possibly, it does not. It can just do what the government proclaims. The actual issue is whether it could be used to perform surveillance in case of any change in priorities, change of authority, or other issues in the sense that the purpose of the app may evolve over time. In security design, intent is less important than capability. Intent may be modified overnight, whereas the capabilities that are built-in are difficult to remove.

This is why there is no bargain on technical transparency. In its absence, we are left only with believing that the government is not going to abuse effective surveillance apparatus. Trust is not enough. Democracies need to be checked, supervised and made accountable. The lack of technical transparency offered by the government to Sanchar saathi is a move that contradicts what the government claims itself to be about the extent of the app.

6. THE MANDATE MECHANISM

6.1 Unpacking the Three-Point Order

The government order of December 2024 requiring Sanchar saathi has three particular requirements, all of which have serious implications.

Point one would mean that every smartphone sold in India will need to be installed with Sanchar Saathi. This poses challenges in the short run in supply chains to the device manufacturers. Firms such as Samsung, Xiaomi, Apple, and others market phones in the world market with rather standard software setups. They now need to develop India specific versions with government imposed apps being added to the bottom layer installation. This adds up expenses, logistics are complicated, and there are possibilities of delays.

The closed ecosystem is something that Apple is struggling with. The firm never gives third-party applications a chance to be pre-installed, particularly, a third-party application that the company has not thoroughly vetted. Allowing this exemption of India may be a precedent where other nations may seek the same treatment of their favorite applications. In the past, Apple has fought these appeals on the grounds that, to preserve a uniform user experience and level of security, it needs to have control over what is shipped with the devices.

In the case of Android manufacturers, pre-installation is technically simple but other issues are involved. Android is already equipped with a number of Google applications. Adding Sanchar saathi is another application that a user cannot easily delete, another application that will consume resources, another application that may gain access to data. The manufacturers are also afraid of the backlash of the users and in particular those consumers who care about their privacy and avoid using obligatory government apps.

And there is history to take into consideration. Phones are usually pre-equipped with alarm systems that alert in cases of an emergency. Such applications can deliver messages of the occurrence of natural tragedies, terrorist acts, or other threats that are on the verge of happening. The reason is understandable, during a crisis, every second matters, and citizens should be notified immediately. However, emergency alert systems are normally very limited. Messages are received and displayed to them. They do not ask massive permissions or operate in the backdrop. They don't collect user data. Sanchar saathi is qualitatively different.

Point two provides that Sanchar saathi is not to be concealed or confined. It should be easily accessible following the installation of the device and its capabilities should not be restricted. This condition places a direct contradiction to the position of the government that the app is optional and that it can be cancelled.

When the application has to be exposed, and its capabilities are not to be restricted, what will deletion mean. Is it possible to delete the app in its entirety, without any traces being left on their devices. Or can they disable it, conceal the icon, but leave the software behind it. This difference is critical. Even when they are not visible to the user, disabled applications may still be able to access data and run background processes and perform functions. True deletion is where the app is deleted altogether, thus destroying its capabilities.

The sentence functions should not be restricted leaves more questions. Is that to say that the app must always be granted the permissions it is seeking. Is it possible to only selectively block permission to enable access to the internet but not location tracking such as. In case users are allowed to limit permissions, is this a limitation of functions. In the event that they are not able, then why is the app optional.

The technical fact is that in the current operating systems such as Android and iOS interface, users are usually able to manage app permissions on a case-by-case basis. You are able to install an app and reject it the right to access location, contacts, storage, or other very sensitive information. However, in case the function of Sanchar saathi has to be limited by the mandate, it means the application has to be granted all the requested permissions. That is what radically alters the essence of optional. An app that you are forced to have installed and which you cannot, in any meaningful sense, constrain, is not in any real sense discretionary.

The third point will expand the mandate to devices that are already in use by updating the software. Sanchar saathi must be made available to all the existing smartphone users within the 90-day implementation window. This is a retroactive demand that is very aggressive.

The updates in the software are optional. They can be installed by users or left in the background in case the user is content with the existing setup. However, phone manufacturers will frequently include security patches, bug fixes and new features in the same update. Declining an update would be to do without valuable security enhancements. The user has a coercive option wherein they can either submit to the Sanchar saathi or they can choose to keep their device exposed to established security vulnerabilities.

The 90 day schedule is extremely quick. Usually, telephone manufacturers do not mind update plans even months before. They have to test the updates on various models of devices to be compatible. They should liaise with carriers that tend to make their own changes. The fact that this process is being compressed into 90 days makes quality a concern. Is the testing of the updates done properly. Will they bring bugs, crashes or compatibility problems. The hurry implies that compliance is put in the first place, and user experience is in the second.

Forced apps updates have been demonstrated to be dangerous by international precedents. Manufacturers found it difficult to install some apps offered by Russia as required, and keep their devices safe at the same time. Part of the functionality was broken in some of the updates. There were security deficiencies that were unintentionally created by others. Users complained of performance slowdown, battery life reduction and unexpected behavior. These were not deliberate sabotage but just random effects of the software alterations that were rushed and had political reasons.

The mechanism of the mandate shows the way in which governments may utilize the technical requirements in order to meet the political objectives. The government can determine which devices can be used with

devices by controlling who can use them, by enabling visibility and open functionality, by compelling upgrades on currently used devices, which amounts to the government obliterating user choice, under the pretence of optional installation.

This is important as individual control is control over Internet autonomy. The phone is the nearest item of technology that majority of people own. It is aware of where you are, to whom you are talking to, what you are reading, what you are purchasing, what you are researching and what you are worrying about. It gets into your bank accounts, your health records, your communications and your entertainment. A basic claim of government authority over the privacy of digital space is to insist that any such device should have a government app that has extensive permissions and limited restrictions in its functionality.

The requirement would not be so troublesome with very strong laws in place. In the event of stringent restrictions on the kind of information that may be gathered, the way it may be utilized, the duration of its object of action and accessibility to people, by imposing controls to monitor what is done and severe consequences of breach of the regulations. India does not have such safeguards. The mandate generates power without responsibility, freedom without inhibition.

7. THE REVERSAL DEMOCRATIC ACCOUNTABILITY IN ACTION

7.1 The 24-Hour Policy Cycle

One of the fastest reversals of the major policies in the recent Indian governance is the Sanchar Saathi mandate reversal. The analysis of the timeline will help us to comprehend in what place the democratic pressure occurred and how the government reacted.

Day 1- Morning: Mandate Announced

It was a directive of the Ministry of Electronics and Information Technology. It mandated all smartphones being sold in India to be pre-installed with Sanchar Saathi. The implementation window was 90 days in case of new devices and the updates had to be made on existing devices.

Day 1 Afternoon to Evening: Popular Protests Grow

The social media burst with both left and right sides of the political spectrum. The technical justification was attacked by tech journalists. Constitutional risks were cited by the proponents of privacy. The normal citizens were concerned about the enforced government application. Industry actors, particularly Apple, indicated opposition.

Day 2 – Morning: Policy Reversed

The reversal was announced by a press release. It was said by the government that Sanchar Saathi was becoming more and more accepted as it registered 600,000 new subscribers in a single day, which was ten times more than before.

7.2 Analyzing the Government's Justification

The argument by the government is worth questioning. It said Since Sanchar Saathi continues to gain acceptance, we will not make pre-installation mandatory to manufacturers.

Statistical Reality Check:

- 600,000 registrations is approximately 0.05 per cent of the 1.2 billion mobile users in India.
- That spike was during a time of very high controversy implying it was not popular interest but investigational.

- The growth a thousand times on a small base does not indicate mass acceptance.
- There is no comparison of other voluntary government-app uptake rates.

Logical Inconsistencies:
In case voluntary adoption had any significance, why did the mandate have to be in the first place. The reasoning undermines the initial assumption. It may be interpreted as either the security menace was much overstated, or the security menace exists but is not taken voluntarily. The most probable interpretation the confronted with the opposition of an undivided opposition, the government chose to withdraw and save its own image considering the move a victory.

7.3 What the Reversal says about Democratic Mechanisms

Public Voice Matters:
Quick reversal indicates that vocal opposition by the citizens has some weight in a democracy. Media-social amplification, news reporting, commentary by experts and civil doubt established political expenses that the government could not slough over.

There was considerable suspicion in the comment of the people:

- They can deceive the old generation with them figures not all.
- "It is a method of monitoring the activities of people.
- Why so now this government so concerned.
- Allusions to the Pegasus spyware scandal highlighted previous concerns about surveillance.

Those suspicions were not paranoid they were contextual based on previous controversial issues and trends of international surveillance.

The Resistance to the Industry Provides Leverage:
The privacy principles of smartphone manufacturers, in particular, Apple, are high. The non-pre-installation of the app by Apple led to a compliance crisis. India could have thought of banning iPhones or delaying imports or creating hindrances, however, these alternatives were all costly. The government realized that the politically valuable aspect of the mandate would be outweighed by the fact that it would be fighting a giant technological corporation in the view of the people.

Speed of Reversal Indicates Decision Calculus:
The 24 hours turnaround implies a calculated cost-benefit analysis. Prolonged debate would have:

- Burnt tech-government credibility.
- Federal litigation called appeal under the 2017 privacy decision.
- Scrutiny by foreign eyes on the issue of surveillance.
- Disaffected tech-industry associates.
- Organized opposition on privacy.

Fast turnarounds reduced such damages and saved face.

7.4 International Reactions and Precedent-Setting

The episode received worldwide attention as a test case of:

Democratic Surveillance Republicanism:
Other emergent democracies monitored. The turnaround of India demonstrates that people in countries that are not very secure yet are populated do not want their state to have them compulsory in the form of obligatory applications.

Industry Standards:
The opposition of Apple solidified its privacy policy around the world. The fact that manufacturers are able to circumvent national requirements in large markets gives them more force to their arguments against such moves in other countries.

The effectiveness of the CSO is excellent, and the organization is perceived as very effective it possesses a highly developed image, reputation, and policies.<|human|>Civil Society Effectiveness:

Government backlash mobilised within seconds was capable of changing policy in response to a security-justified action. This empowers similar movements in other places.

7.5 What the Reversal Doesn't Solve

Even though it shows an element of democratic accountability, there are numerous fundamental issues:

There are still Legitimate Security Concerns:

- Secondhand markets in phones are flooded with stolen phones with falsified IMEIs.
- Customers have no effective checks prior to buying.
- Digital fraud is rising.
- Co-ordination amongst law enforcement, telecoms and consumers is disjointed.

No Area of Alternative Solution Presented:
The government retracted the requirement but provided no alternative to take care of the initial security purpose. Possible reasons:

- The risk is over-rated and therefore does not demand any solution.
- There exist other methods which are not prioritized.
- Mandatory installation can be revisited with new framing on the part of the government.

Remains Infrastructure Capability:
Sanchar Saathi continues to operate with its requested permits. Those capabilities are maintained by voluntary downloads. Technical architecture, which has any surveillance possibility, remains the same.

Trust Deficit Deepens:
The episode intensified the doubt regarding technology projects by governments. New venerable security policies can be challenged more because of diminished trust. The citizens will not accept the trust us without transparency, independent verification and legal protection.

Continues to Lack Gap in Regulatory Framework:
India does not yet have an extensive law on the protection of data. The reversal did not bring about an immediate crisis but still had not established the framework that would prevent future overreach of surveillance or maintain the safety of citizen data exchanged with the government apps.

7.6 Lessons for Future Digital Governance

The Sanchar Saathi turnaround provides some lessons:

For Governments:

- Mandatory state applications having general permissions raise an immediate suspicion.
- Rollout should be preceded by technical transparency and independent audits.
- Without checking, there are assurances of trust which do not work in democracies.
- Posing security measures as a choice and a prerequisite creates cynicism.
- Rapid change of policy can minimize the harm of political mistakes.

For Citizens:

- Organized, relentless opposition succeeds.
- Resistance is fueled by technical literacy of app permissions.
- The mention of constitutional rights makes them stronger.
- Political pressure is created, through social-media amplification.
- Citizen leverage is increased by industry allies that do not comply.

For Technology Companies:

- Privacy precepts vary and inject a sense of value in the market.
- Opposition to overreach can be effective in the case where the costs of compliance exceed the benefits.
- User privacy protection is well received by the companies.
- International norms (e.g., that of Apple) serve as an advantage in domestic conflicts.

For Civil Society:

- Compelling response to threatening policies prevents normalization.
- Specialist technical analysis provides details to the masses.
- Constitutional systems provide a legal foundation of resistance.
- Domestic pressure is magnified by international attention.

8. THE PRIVACY ARGUMENT

8.1 Why Opposition Voices Are Concerned

The opponents of Sanchar saathi are not only concerned with partisan politics. They use the constitutional concepts, past experiences, and the technicalities of the surveillance infrastructure, as a foundation to their argument.

Begin with the constitutional system. In 2017, the Supreme Court of India made a historic decision in Justice K.S. Puttaswamy (Retd.) vs. Union of India, pronouncing privacy a fundamental right in Article 21 of the Constitution. The court formed privacy to consist of informational privacy (control over personal data), bodily privacy, and privacy of choice. It established certain tests that any government intervention that violates privacy should meet.

First, the act should seek a valid political purpose of the state. Second, one must have a reasonable relationship between the means selected and that end. Third, it has to be proportionate, i.e. no alternative that is less intrusive can have the same objective. Fourth, the protocols should guard against abuse.

These critics claim that Sanchar saathi does not pass these tests. Although cybersecurity is a valid cause of state, requiring pre-installing an app with surveillance capabilities is unreasonable when there are less invasive alternatives. The same security objectives can be met using voluntary downloads, web-based reporting, enhanced law enforcement, and enhanced user education instead of compelling everyone to install government software in personal machines.

Of particular interest is the absence of procedural safeguards. Sanchar saathi does not have any independent control over its operation. Privacy impact assessment is not published. Legal boundaries that might stop the weaponry developing into ubiquitous watching framework are nonexistent. Misuse does not have any significant punishments. The absence of these safeguards makes the mandatory installation unconstitutional.

The question on the data collection is not answered. What is the information that Sanchar saathi collects. The government claims that it does not engage in access to personal information or in interception of communication. However, what are personal data in this case. Does location history count. Call logs. App usage patterns. Data on your communications, no content. No personal data claims have no meaning without clear documentation.

More essentially, what happens to gathered information. Does it reside on your computer or is it sent to the government computers. Is it encrypted during transmission should it be. What is the location of the servers. Who has access. How long is data retained. How do the government bodies get access to it through legal procedures. Is it transferable to other nations. These are not paranoid questions, but simple necessities of any system that gathers the data of citizens.

The issues are highlighted by historical context. Surveillance infrastructure has been frequently abused by governments of the world and most of these programs started small and well-meant but grew in size. Mass surveillance programs by the United States NSA began to be narrowly aimed at fighting terrorists, but expanded to include mass interception of communication by millions of non-terrorists citizens. The surveillance infrastructure of China was originally advertised as the crime prevention tool but developed into the system of enormous social control. The need of communication monitoring that Russia had was based on the level of security threats but has now been expanded on to political dissent.

The precedents in India are of concern by themselves. Pegasus revelations indicated that journalists, activists, opposition politicians and members of the civil society were targeted using advanced spyware. Although the government denied its role, independent investigations proved that Indian phone numbers were found on lists of the possible targets, proving both the possibility and readiness to carry out the surveillance operations which were not related to the reasonable security needs.

The COVID Aarogya Setu experience was also raising red flags. The application was a compulsory requirement in most operations even though it was technically optional. The assurance came with regard to questions concerning the security of data, not transparency. Finally, they failed to enforce promised restrictions on data retention. The health tracking infrastructure would be easily used in other monitoring.

These concerns are supported by international examples. Health code apps which were originally designed to track the COVID outbreak in China have become converts which will continuously limit the movement of

citizens depending on their social credit rating and political trustworthiness. The compulsory apps in Russia became the pandemic response instead of the overall surveillance. When infrastructure is constructed, it is unlikely to be destroyed and its uses are likely to increase.

Another critic of privacy is the power imbalance behind such a system. A single citizen does practically not have a bargaining position in the case of state surveillance. The government cannot be bargained on what data it is gathering, the audit mechanisms to check or confirm compliance and there is no meaningful redress should your data be misused. The interaction between the state and people is categorically unequivocal the state possesses complete information knowledge, and people only have information that the state wishes to reveal.

This imbalance is threatening in any form of democracy but more so in a moment where institutions are weak, press freedom is limited or political polarization is on the rise. The possibility of abuse is enormous when the governments are able to monitor the citizens on a broad basis. Dissent can be chilled. Opposition can be targeted. Discrimination may take place against minorities. And in the process keeping a fiction of being lawful.

It is not entirely inaccurate, although possibly hyperbolic in degree, to say that the comparison with North Korea is correct. North Korea has laws requiring state-tracking applications that keep the state informed about the communications, movements and activities of the citizens at all times. The apps are not removable or disabling and they have unlimited access to the functionality of the device, the citizens are not privacy-aware, cannot make a choice or take action against misconduct.

Sanchar saathi is by no means the same. India is a constitutional democracy that has constitutional safeguards, powerless judiciary and a rich civil society. The technical architecture is not different it is mandatory, unrestricted, broad permissions, minimal transparency. This dissimilarity is not in the abilities of the tool, but in the institutional limitations of its application. In case those constraints become weaker, in case the democratic norms are undermined, in case the political situation also shifts, the infrastructure of all-inclusive surveillance already is in place.

This is the reason why critics claim that capability is not as important as intent in measuring the surveillance systems. Sanchar Saathi, perhaps, truly aims at cybersecurity by the current government. But capabilities once constructed outlive the intent of a certain government. This infrastructure will be passed on to future administrations who may experience various pressures or temptations. It should not even be constructed at best, on the hope that it will never be abused.

There is the basic privacy point of view which is that, democracies must make errors favoring civil liberties at the expense of security. There is no such thing as perfect security dilemmas and in many cases when one tries to achieve this, it results in authoritarianism. There is a freedom of price that involves a certain degree of risk. India does have actual cybersecurity issues, but its response to them by implementing obligatory surveillance infrastructure puts the Indian society at risk to something even more valuable than security the very democratic nature of the Indian society.

9. CONCLUSION

The Sanchar Saathi mobile app is a turning point in the Indian system to strike a balance between national security and constitutional concerns regarding privacy. It reveals fundamental contradictions that will determine digital governance in the biggest democracy on the planet. The program was originally an honest

attempt to address the issue of mobile phone theft, counterfeit IMEI numbers, and criminals using SIMs. It became a constitutional stand-off as authorities attempted to impose an obligatory installation, preventing banking services and restricting recharge services. The government took a turnaround in 24 hours of the December 2 directive following the widespread public outcry on social media and intervention of opposition leaders. This indicates that democratic accountability is successful when citizens mobilize against what they consider to be overreach of surveillance. However, the triumph is partial and perhaps pyrrhonist. Cybersecurity is an actual issue in India approximately 40M stolen devices annually, an unregulated gray market that sells copied IMEI numbers, a highly advanced cyber-fraud targeting digital transactions, and millions of buyers who are not able to check the authenticity of their device. The inability of the government to stand ground on the objective of 600,000 voluntary registrations by citing it as the rising number of voluntary use as an indicator of rising acceptance showed that there was a major weakness in this strategy of forced implementation. This episode intensifies, but not concludes the tension between the capacity of technology and the constitutional restrictions. The Puttaswamy judgment of 2017 ensured that privacy is a right and required that any decisions by the government must be proportionate, necessary, and procedurally protective. However, the Sanchar Saathi requirement proceeded with no debate on a legislative level, no independent audits, and no obvious data-protection measures. Practical solutions would include strong privacy laws which have enforcement mechanisms, independent regulatory bodies with actual authority (not advisory) enforced in all government technology projects, privacy-by-design, and funding privacy-conservative alternatives (which may include blockchain-based IMEI registries, decentralized authentication, fraud detection in the network, which identifies threats without surveillance), and even stronger regulation to address device theft and IMEI cloning. The overturn demonstrated one of the most important rules that are often overlooked in the security discourse capability is more important than intent. After constructing the surveillance infrastructure, it would remain when the government alters its commitments. It is open to mission creep, can be exploited for political purposes, and can be redefined according to new principles of legitimate use. India has a real dilemma to follow its current path of surveillance intensive security policies that people will not submit to, or to invest in privacy preserving technologies that will generate trust among the people by establishing transparency, upholding constitutionality, and providing democratic accountability. India has 1.2 billion mobile subscribers with a fast rate of digitization the course that the country takes will set the world standards on how the state can snoop, digital rights and the connections between security and liberty in democracies. This event demonstrates that the citizens have a chance to refuse to use mandatory state surveillance apps, but constant attention is crucial. Democracies cannot naturally build self-defense and hence require active, deliberate involvement that refuses to make false binary decisions between security and freedom, protection and privacy as mutually supporting, and hold governments accountable when technology becomes dangerous to constitutional boundaries.

REFERENCES

[1] Sadiq AA, Dougherty RB, Tyler J, Entress R. Public alert and warning system literature review in the USA: identifying research gaps and lessons for practice. Nat Hazards (Dordr). 2023;117(2):1711-1744. doi: 10.1007/s11069-023-05926-x. Epub 2023 Apr 11. PMID: 37251347; PMCID: PMC10098234.

[2] Dr.A.Shaji George, Dr.T.Baskar, Dr. P. Balaji Srikaanth, & Dr.M.M.Karthikeyan. (2025). Building Resilient API Security Through a Five-Dimensional Framework for Data Breach Prevention in Modern Digital Ecosystems. Partners Universal Multidisciplinary Research Journal (PUMRJ), 02(04), 32–50. https://doi.org/10.5281/zenodo.15862111

[3] Age, A., Age, A., & Asian. (2025, December 2). asian. Asian. https://www.asianage.com/opinion/edit/aa-edit-sanchar-saathi-security-vs-liberty-or-govt-overreach-1921167

[4] Agencija. (2017, June 15). GASI SE FK NOVI PAZAR! Klub proglasio bankrot zbog velikih dugova! Sandžak PRESS. https://sandzakpress.net/arhiva/gasi-se-fk-novi-pazar-klub-proglasio-bankrot-zbog-velikih-dugova/comment-page-1/.s-news-16067357-2025-12-02-india-mandates-pre-installation-of-govt-cybersecurity-app-on-all-smartphones-sparking-privacy-concerns

[5] Bhalla, V. (2025, December 3). Where Sanchar Saathi stands on user consent, constitutional test on privacy. The Indian Express. https://indianexpress.com/article/explained/explained-law/where-sanchar-saathi-stands-on-user-consent-constitutional-test-on-privacy-10399165/lite/

[6] CENTEGIX. (2024, February 22). CENTEGIX CrisisAlert: Every second matters [Video]. YouTube. https://www.youtube.com/watch.v=UWTVevwP3xg

[7] Chronicle, D., Chronicle, D., & Chronicle, D. (2025, December 2). Deccan Chronicle. Deccan Chronicle. https://www.deccanchronicle.com/opinion/dc-comment/dc-edit-sanchar-saathi-security-vs-liberty-or-govt-overreach-1921169

[8] Data protection laws in South Korea - Data Protection Laws of the World. (n.d.). https://www.dlapiperdataprotection.com/.t=law&c=KR

[9] Desk, T. W. (2025, December 1). India pushes for mandatory pre-installed cybersecurity app on all new smartphones. The420.in. https://the420.in/india-smartphone-preinstall-order-apple-privacy-cybersecurity-crackdown/

[10] Desk, W., & Madhyamam. (2025, December 3). The mysterious entry of Sanchar Saathi. Madhyamam. https://madhyamamonline.com/opinion/editorial/the-mysterious-entry-of-sanchar-saathi-1473347

[11] Donnelly, S. (2025, December 3). India reverses mandatory cybersecurity app after Apple privacy concerns. WebProNews. https://www.webpronews.com/india-reverses-mandatory-cybersecurity-app-after-apple-privacy-concerns/

[12] Edge, S. (2025, December 3). Sanchar Saathi Mandate: Security vs. Privacy in the Age of Digital Arrest. STRIVE IAS ACADEMY. https://striveedgeias.in/sanchar-saathi-mandate-cybercrime-privacy-puttaswamy-proportionality/

[13] George, D. (2024). Personal privacy at risk: The security threats of sharing boarding passes online. Zenodo. https://doi.org/10.5281/zenodo.14503012

[14] Enable or disable background apps in Windows 11. (2021, August 10). Windows 11 Forum. https://www.elevenforum.com/t/enable-or-disable-background-apps-in-windows-11.923/

[15] European Union - Data privacy and protection. (n.d.). International Trade Administration | Trade.gov. https://www.trade.gov/european-union-data-privacy-and-protection

[16] George, D. (2025). An exploratory study of friendship marriage and its role in redefining partnership for economic security and personal autonomy in modern society. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.17137271

[17] Ghosh, A. (2025, December 2). Sanchar Saathi Controversy explained: Why a phone security app sparked India's biggest privacy row. Times Now. https://www.timesnownews.com/india/sanchar-saathi-controversy-explained-why-a-phone-security-app-sparked-indias-biggest-privacy-row-article-153237266

[18] George, D., Dr.T.Baskar, & Srikaanth, P. B. (2025). Bridging the Security Skills Gap: A comprehensive framework for developing application security competencies in modern software engineering. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.15616416

[19] Hacks, G. (2025, December 2). India orders Apple to install Gov't app on all iPhones. Gadget Hacks. https://apple.gadgethacks.com/news/india-orders-apple-to-install-govt-app-on-all-iphones/

[20] Inamdar, N. (2025, December 3). Sanchar Saathi: India scraps order to pre-install state-run cyber safety app on smartphones. https://www.bbc.com/news/articles/clydg2re4d1o

[21] George, D., & Dr.T.Baskar. (2025). Security and privacy comparison of Arattai, WhatsApp, and WeChat: India's messaging app landscape and digital sovereignty. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.17483067

[22] India Demographics 2025 (Population, Age, sex, Trends) - Worldometer. (n.d.). Worldometer. https://www.worldometers.info/demographics/india-demographics/

[23] India orders preinstall of security app, critics warn of mass surveillance. (2025, December 3). CHOSUNBIZ. https://biz.chosun.com/en/en-international/2025/12/03/AIXVHHBDB5DDHOQ2SP6LWSCTWM/

[24] George, D., Dr.S.Sagayarajan, Baskar, D., & Pandey, D. (2024). Assessing the security and privacy implications of India's DigiYatra initiative. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.14599297

[25] India Today. (2025a, December 2). Mandatory Sanchar Saathi: Can the cybersecurity app become a surveillance tool. https://www.indiatoday.in/india-today-insight/story/mandatory-sanchar-saathi-can-the-cybersecurity-app-become-a-surveillance-tool-2829505-2025-12-02

[26] India Today. (2025b, December 2). Mandatory Sanchar Saathi: Can the cybersecurity app become a surveillance tool. https://www.indiatoday.in/india-today-insight/story/mandatory-sanchar-saathi-can-the-cybersecurity-app-become-a-surveillance-tool-2829505-2025-12-02

[27] Kugelman, M. (2025, April 2). India faces high stakes in U.S. trade talks. Foreign Policy. https://foreignpolicy.com/2025/04/02/india-us-trade-talks-deal-reciprocal-tariffs-trump/

[28] Mishra, A. (2025, December 2). India makes Sanchar Saathi mandatory on all new smartphones sold in the country. Organiser. https://organiser.org/2025/12/02/328498/bharat/india-makes-sanchar-saathi-mandatory-on-all-new-smartphones-sold-in-the-country/

[29] NH Digital, & Digital, N. (2025, December 1). Indian govt wants smartphone makers to preload State-owned app: Report. National Herald. https://www.nationalheraldindia.com/national/indian-govt-wants-smartphone-makers-to-preload-state-owned-app-sanchar-saathi-report

[30] Northlines. (2025, December 3). 'No snooping, no forced use': SCIndia defends Sanchar Saathi App. Northlines. https://thenorthlines.com/no-snooping-no-forced-use-scindia-defends-sanchar-saathi-app/

[31] Online, E. (2025, December 2). Sanchar Saathi app controversy explained: Why the govt is pushing this 2-year-old tool, how it works, and. The Economic Times. https://economictimes.indiatimes.com/news/india/sanchar-saathi-app-controversy-explained-why-the-govt-is-pushing-this-2-year-old-tool-how-it-works-and-why-users-are-worried/articleshow/125714329.cms.from=mdr

[32] Reporter, G. S. (2025, December 2). India orders phone makers to preload devices with state-owned cyber safety app. The Guardian. https://www.theguardian.com/technology/2025/dec/01/india-phone-sanchar-saathi-app-cybersecurity

[33] Rodriguez, E. (2025, December 5). India Reverses Smartphone Mandate, Drops Pre installation Order for Sanchar Saathi. Prism Media. https://www.prismedia.ai/news/india-reverses-smartphone-mandate-drops-pre-installation-order-for-sanchar-saathi

[34] Sanchar Saathi app requirement cancelled as public outrage forces govt u-turn. (n.d.). Moneylife NEWS & VIEWS. https://www.moneylife.in/article/sanchar-saathi-app-requirement-cancelled-as-public-outrage-forces-govt-uturn/79023.html

[35] Siddiqui, U. (2025, December 3). Why did India order smartphone makers to install a government app. Al Jazeera. https://www.aljazeera.com/news/2025/12/3/why-did-india-order-smartphone-makers-to-install-a-government-app

[36] Srinivasan, S. (2025, December 2). UPSC Daily News summaries: essential current affairs, key issues and important updates for civil services | Hindustan Times. Hindustan Times. https://www.hindustantimes.com/education/upsc-daily-news-summaries-sanchar-saathi-cyclone-ditwah-winter-session-parliament-sir-venezuela-ukraine-russia-101764646802485.html

[37] Stephen N R, & Stephen N R. (2025, December 1). India's new mandatory cyber safety app rule: What users need to know. Gulf News: Latest UAE News, Dubai News, Business, Travel News, Dubai Gold Rate, Prayer Time, Cinema. https://gulfnews.com/world/asia/india/india-s-new-mandatory-cyber-safety-app-rule-what-users-need-to-know-1.500365648

[38] taxtmi.com (A unit of MS Knowledge Processing Pvt. Ltd.). (n.d.). Govt withdraws mandatory pre-installation of Sanchar Saathi app on mobile phones | TaxTMI. TaxTMI. https://www.taxtmi.com/news.id=63474&allSearchQueries=

[39] TOI News Desk. (2025, December 2). "Snooping app" charge: Massive political row over Centre's Sanchar Saathi App on mobiles dictum; controversy explained. The Times of India. https://timesofindia.indiatimes.com/india/snooping-app-massive-political-row-over-centres-sanchar-saathi-app-on-mobiles-dictum-controversy-explained/articleshow/125709516.cms

[40] Dr.A.Shaji George. (2025). Digital Watermarking in Cloud Environments for Copyright Protection: A Comprehensive Review. Partners Universal Multidisciplinary Research Journal (PUMRJ), 02(06), 54–74. https://doi.org/10.5281/zenodo.17726895

[41] Valeria, X. (2025, December 3). India's Sanchar Saathi app controversy and its impact on tech and telecom sectors. Ainvest. https://www.ainvest.com/news/india-sanchar-saathi-app-controversy-impact-tech-telecom-sectors-2512/

[42] Wikipedia contributors. (2025, May 24). Security dilemma. Wikipedia. https://en.wikipedia.org/wiki/Security_dilemma