AL-HAYAT Research Journal
HJRS HEC Journal Recognition System
Category Y
Volume 4 Issue 1 (Oct-Dec 2026)
ISSN (Online): 3006-4767
ISSN (Print):: 3006-4759

Privacy vs surveillance: Legality of mobile phone tracking by legal authorities in Pakistan

Bajeel Ameen Babar
Department of Law, Dadabhoy Institute of Higher Education, Pakistan bajeelameen8@gmail.com
Dr. Tansif Ur Rehman
Teaching Associate, Department of Sociology, University of Karachi, Pakistan; and Visiting Faculty, Department of Law, Dadabhoy Institute of Higher Education, Pakistan
tansif@live.com
https://orcid.org/0000-0002-5454-2150

Abstract

The growing number of state institutions in a mobile phone tracking system has been rising while privacy and surveillance has become an important issue in legal and constitutional framework of Pakistan in relation to mobile phone tracking system. All of these digital monitoring, call data records, geo-location and communications interception features are a vital part of the investigations in crime prevention and national security for law enforcement officers. The present research critically discusses the legality of mobile phone tracking by the Pakistani police according to the provisions of the Prevention of Electronic Crimes Act (PECA) 2016, Investigation for Fair Trial Act (IFTA) 2013.

Keywords: challenges, historical context, laws, opportunities, theoretical context.

Introduction

One of the most popular devices deployed by the police or intelligence agency in Pakistan is mobile phone tracking devices. The technological databases such as digital monitoring systems, geo-fencing apparatuses and biometric SIM card and call data records help all the law enforcement authorities to track down criminals and protect national security interests. The protection of the dignity of the man and the private freedom of residence has been clearly expressed in Article 14 of the Constitution of the Islamic Republic of Pakistan, and the Supreme Court has always interpreted it as having included rights of personal life, autonomy of the body and the privacy of letters and correspondence.

Under Article 14 of the Islamic Republic Pakistan (IRP) Constitution, the dignified dignity of the man and the right to private life guaranteed under Article 14 the constitutional constitution of Islamic Republic Islam (IRC) was consistently held as an equivalent of the right for personal life, right to control the body and right to confidentiality of correspondence. As a reaction to this, national security vs civil Liberty debate has come out, and it has been more robust and intensified since the implementation of new and advanced technologies of digital communication in recent times has begun.

Research Justification

The significance of this research is that digital surveillance and mobile phone tracking has harmful impact on the rights of the constitution, democratic systems and people's trust on the state of Pakistan. A careful study of the powers of surveillance as contained in the laws is needed to examine the extent in which Effective protection for individual privacy is provided and how this supports proper investigations.

Literature Review

In their research, Ahmed and Habib (2026) discuss why Pakistani citizens are particularly susceptible to contemporary forms of digital invasion from Article 14 in the Constitution of Pakistan. Likewise, Zaib et al. (2025) argue that the state's power to intercept communications and track mobile devices should be subject to strict and judicious limits to avoid the erosion of individual privacy rights. Jamil (2021) explores the issue of state surveillance in Pakistan, explaining the extent to which state surveillance with the help of communications monitoring and digital tracking enabled by PECA infringe on privacy on a massive scale.

The Prevention of Electronic Crimes Act (PECA), 2016 is also a crucial legal aid for investigations of electronic crimes, as a countermeasure to digital threats (Yongmei & Afzal, 2023). But, Aman et al. (2026) argue that PECA is not able to strike a balance between cybercrime law enforcement and freedom of internet expression as guaranteed by the Constitution. These are the challenges posed to the state power by those who attempt to question the constitutionality of surveillance technologies and caution against the use of national security powers to trample on individual privacy rights.

CC BY

In this context it is argued that the state's surveillance measures should be strictly observed in accordance with the principle of necessity, proportionality and transparency (Sethi et al. 2025). Building on contemporary tracking methods, Soomro et al. (2025) lay out the important drawbacks of AI-assisted policing such as algorithmic bias and data profiling.While, Elif (2026) argues the necessity of implementing enforceable constitutional restrictions and judicial autonomy to prevent the unchecked digital surveillance of citizens in Pakistan.

Historical Context

As the national security concerns in Pakistan, Counter Terrorism operations and technical modernization have evolved, the evolution of surveillance laws can be observed. Historically, the capacity to monitor people's activities relied on physical intelligence and on tried-and-tested wiretapping, which has been legalized since colonial times in the telecommunication laws. In the era of geopolitical change after 2001 and the emergence of digital telecommunications, the digital surveillance apparatus of intelligence and law enforcement agencies, in particular, has greatly expanded.

In order to provide statutory guidelines for electronic surveillance, Pakistan has introduced certain legislations such as the Investigation for Fair Trial Act (2013) and Prevention of Electronic Crimes Act (2016). These laws created legal avenues for the collection of digital evidence, monitoring of cell phones and electronic communications under certain circumstances. Even so, human rights activists and legal professionals are still concerned about the lack of independent monitoring by police of their actions.

Theoretical Context

The prism of theory and debate on privacy and surveillance is one in which the public good of security is weighed against the individual's rights. Private life, as a cornerstone of human rights in constitutional and liberal democratic theory, is essential to maintain human dignity, personal liberty and unencumbered freedom of expression. Such unchecked and unsupervised surveillance undermines this balance by fostering an atmosphere of terror within institutions, cracking down on legitimate dissent, and eroding the democratic norms and foundations. Security and public interest arguments, however, underpin the surveillance as a way of countering the threat of terrorism, of tackling organized crime and of addressing the new challenges of cyber warfare. Theories of modern constitution have taken the middle path by incorporating the doctrine of "proportionality" which is based on the premise that any limitation on communications privacy must have a clear statute, pursue a legitimate security interest, and be judiciously challenged by courts.

Relevant Laws

1. Prevention of Electronic Crimes Act 2016 (PECA): this act allows for the regulation of cybercrime crimes and gives the State statutory powers in the field of digital forensics, electronic data retention, search, seizure and investigations of cybercrime.
2. Investigation for Fair Trial Act 2013 (IFTA): outlines the process for lawful interception and electronic surveillance in the course of national security investigations, such as the requirement to get a warrant from the Justice Department before any interception or electronic surveillance can take place.
3. According to Article 14 of constitution of Pakistan 1973: dignity and privacy of home is a fundamental right and will be guaranteed along with the right to due process and fair trial as provided in Article 4 and 10A, respectively.
4. Pakistan Telecommunication (Re-organization) Act, 1996: Telecommunication licensing, telecommunication infrastructure services and legal obligations of telecommunication infrastructure services with telecommunication services providers and government departments in respect of interception of telecommunication services for national security purposes.
5. Pakistan Penal Code, 1860: Provides criminal penalties for unauthorized access to data, unlawful interception and harassment.

Challenges

However, it appears that the government is operating in the dark in Pakistan in case of mobile devices. No one tells normal people that they are being recorded by someone while they are on the phone, and no one tells on normal people they aren't pointing out that data is being taken about them without knowing it. This unabated form of leverage always ends up in the hands of the critics of civic action, and the critics with political objections. Phone monitoring of journalist, human rights activist, courtroom lawyers and opposition politicians is a regular occurrence with the aim of blocking free speech and expression.

What made it even worse, Pakistan has yet to have a law in place to protect personal information and it has not been enforced. No protection whatsoever and no protection for normal Telecom user. Intimate user records are then sold by commercial user record brokers, dumped online or steal by state actors who are beyond the oversight of any agency. Besides that, technology is also becoming more quickly than domestic laws. The deployment of automated facial recognition cameras in public spaces, combined with a centralized biometric database based on national identity cards is being used and there is no good law to control this.

Opportunities

As an under developed country, Pakistan has an obvious opportunity to improve its digital surveillance laws without harming the factual national security needs. The first step would be the enactment of a broad, robust and robust Personal Data Protection law wherein both state ministries and the telecom companies would have a legal duty to manage personal data management.

There is a need to put an end in warrantless snooping. To provide an extra protection against executive overreach, the law enforcement would need to get the judge's authorization to wiretap phone calls, gain access to network traffic and/or track the real-time location of the device. How do you expect agencies to be able to regulate themselves in the open when you can't allow them to control them behind closed doors? How can security agencies manage themselves in the dark, when they can't manage in the light? To further strengthen these protections, the legislators should establish independent bodies under law that have access to records and can make periodic, confidential, secret auditors of these records and who can punish any violation of personal safety in communication. True to his point, it is not a dragnet needed to be effective at policing crime.

Discussion

The mobile phone tracking is one of the rising tension between the rights to privacy and national security aspects in Pakistan. The use of modern tracking technologies is a helpful aid in the investigation of crime and counter-terrorism, and should be done within the confines of the Constitution and the democratic rule of law. There are some statutory mechanisms as outlined in the legislative instruments such as PECA 2016 and IFTA 2013; however, there is no operational compliance and transparency in the implementation of the legislative measures within the framework of civil liberties. Efficient security efforts must go hand in hand with legally binding accountability and transparency in court proceedings for sustainable legal reform.

Conclusion

In Pakistan, privacy and surveillance is an ever-present constitutional and legal question: As the powers of the state to track increases, privacy is becoming a major concern. While electronic surveillance can help to stop terrorism and cybercrime, there are legitimate concerns and fears, particularly about the potential for overreach and underreporting by the Government. There are several areas where the law needs to be improved, as well as how warrants are issued, and institutional accountability to surveillance, in order for surveillance operations to be fully aligned with the constitutional rights and international human rights conventions under Article 14.

Recommendations

A four-part model for a reform is proposed to protect the right of citizens' privacy while maintaining the legitimate investigative powers of citizens. There is a need for an independent law on Personal Data Protection to establish boundaries around the collection, storage and processing of citizens' data and the justification of processing it. Second, all requests for tracking, geo-fencing or interception of mobile phones must be made to a competent court with very few exceptions for cases of real emergency and strictly audited.

Third, there should be an independent Surveillance Oversight Commission made up of judicial experts and technical specialists, which audits intelligence requests and which publishes transparency reports on intelligence annually, thus providing transparency and accountability to the public. Last, training and capacity-building efforts should be conducted for prosecutors, judicial officers and investigators and cover the following: constitutional privacy standards; cyber law; and integrity of digital evidence. The measures put in place all contribute to a well-balanced system of surveillance that is legal, proportionate and accountable.

Research Limitations

There are limitations in this study that could impact the results. But nothing is public about the surveillance activities of the Pakistani government. For example, no details exist of how frequently the government requests surveillance, the number of orders issued for interception or the type of intelligence operations. As much of this information is classified for national security purposes it is hard to determine if the information provided is accurate. It takes longer to be able to keep up with the developments in digital communication and surveillance by means of laws and decisions in court. This may result in uncertainty over privacy rights of citizens and oversight and transparency around government surveillance.

References

Ahmed, M. T., & Habib, R. I. (2026). The Prevention of Electronic Crimes Act, 2016: Balancing cybercrime control and freedom of online expression in Pakistan. *Pakistan Journal of Humanities and Social Sciences, 14*(1), 368–375. https://doi.org/10.52131/pjhss.2026.v14i1.3209

Aman, S., Hussain, Z., & Fatima, K. (2026). Right to privacy under Article 14: How protected are citizens in the digital age? *The Critical Review of Social Sciences Studies, 4*(1), 2995-2999. https://doi.org/10.59075/sb9dmg51

Elif, M. U. (2026). State surveillance without safeguards: Constitutional limits on digital monitoring in Pakistan. *Social Science Review Archives, 4*(1), 6944–6955. https://doi.org/10.70670/sra.v4i1.2559

Jamil, S. (2021). The monitored watchdogs: Journalists' surveillance and its repercussions for their professional and personal lives in Pakistan. *Journalism Studies, 22*(78), 878–895. https://doi.org/10.1080/1461670X.2021.1904272

Sethi, A., Ullah, H. H., & Naseem, R. M. S. (2025). Surveillance, national security and the right to privacy in the digital era. *The Critical Review of Social Sciences Studies, 3*(4), 431–443. https://doi.org/10.59075/gf564d60

Soomro, S. A., Kalhor, H. B., & Gujjar, M. (2025). AI-driven policing in Pakistan: Potential pitfalls, and privacy concerns. *Pakistan Social Sciences Review, 9*(3), 3338-350. https://doi.org/10.35484/pssr.2025(9-III)28

Yongmei, C., & Afzal, J. (2023). Impact of enactment of "The Prevention of Electronic Crimes Act, 2016" as legal support in Pakistan. *Academy of Education and Social Sciences Review, 3*(2), 203–212. https://doi.org/10.48112/aessr.v3i2.500

Zaib, H. U., Shaheen, M. B., & Chaudhary, H. K. (2025). Constitutional validity of surveillance technologies in Pakistan: Reconciling national security with individual privacy rights in the digital age. *Social Science Review Archives, 3*(3), 1653–1665. https://doi.org/10.70670/sra.v3i3.991