

Comparative Analysis of Privacy in Digital Age

V. National Security

Shraddha Agarwal

Bba Llb 5th Year Ims Unison University, Dehradun

Abstract

This paper examines the tension between individual privacy rights in digital era and national security interests. It reviews constitutional and statutory protections, judicial decisions and international guidance. It also identifies the challenges that surveillance policies raise on privacy and data protection. Using comparative case studies from India and other international countries, the paper analyzes legal tests and doctrines that are used by courts to balance the rights to privacy and also national security interests. This paper concludes with recommendations to align national security practices with human rights standards.

Keywords: Right to privacy, national security, digital surveillance, Investigatory powers, Constitutional law, Puttuswamy, Carpenter, International law

INTRODUCTION

In an era where personal data is constantly being collected, data privacy has become one of the most pressing legal and ethical issues of the digital age. Every online interaction or work whether on social media, e-commerce platforms or healthcare portals – creates a digital footprint that governments and also cyber criminals such as hackers can exploit. There is rapid increase in use of artificial intelligence in every field.

Use of internet has increased over the past two decades. Typical data collected from users can include persons' personal information such as person's name, contact number, address and bank related details too. Data breaches can put all the information at risk. Privacy is not a conferred right but a natural one.

It involves respecting an individual's right in private without compelling reason to disclose them. Judge Thomas Cooley provides a fundamental definition of privacy in the case of *Olmsted v. US* referring it as the right to be alone. The growth of the information Technologies role in the society and the widespread use of computers and information processing in public in the last three decades of the 20th century.

The purpose of this article is to present some main challenges of the contemporary digital technologies and online social networks. These technologies have good position in the digital age but could cause problem for realization of the principles of Confidentiality and Integrity. India, having recently enacted the digital personal data protection Act, is in the process of developing a structured framework for data protection.

LEGAL FRAMEWORK AND CORE PRINCIPLES

1. Conceptual overview

The intersection of privacy and national security lies at the heart of modern constitutional and international human rights law. The right to privacy protects the individual autonomy, dignity. National security on the

other hand is an essential function of state aims at ensuring territorial integrity, public order, and protection from internal and external threats

1.1 Constitutional and international basis of Right to privacy

(a) International framework

(a) Universal declaration of Human Rights, 1948- Article 12

No one shall be subjected to arbitrary interference with his privacy, family, home and should not be attacked upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.

(b) International covenant on civil and political rights, 1966- Article 17

Protects individuals from arbitrary or unlawful interference with privacy and requires states to adopt legislative measures ensuring this protection.

(c) European Convention on Human rights, 1950 – Article 8

Sates the right to respect for private and family life, home and correspondence, subject to restrictions necessary in a democratic society for national security, public safety, or prevention of disorder or crime.

(b) Constitutional frame work

1. India - Article 21, Constitution of India

The right of life and personal liberty states the right to privacy as recognized in justice K.S Puttuswamay v. Union of India (2017)

The supreme court declared right to privacy as a fundamental right to human dignity, stating that any limitation must meet the tests of legality, necessity and proportionality.

2. United States- Fourth Amendment to the U.S Constitution

Protects citizens against unreasonable searches. in the case of Carpenter vs. United states (2018), the Supreme court extended these protections to digital data such as historical cell- site location information, stating that long term tracking infringes privacy even in the absence of physical intrusion.

3. United Kingdom – Human rights Act, 1998 and investigatory powers act, 2016

The human rights act incorporates article 8 of the ECHR into domestic law, ensuring respect for private life. The investigatory powers act 2016 provides a legislative framework for lawful interception, data retention, surveillance coupled with judicial oversight through warrants.

1.2 Fundamental legal principles

The reconciliation of privacy with national security in all major jurisdictions is guided by three core legal principles:

(a) Principle of legality

Any restriction on the right to privacy must have a clear and specific legal basis. Laws authorizing surveillance or data collection must be:

- . Accessible to public
- . Precise and foreseeable in their application
- . Subject to independent authorization and oversight

This principle ensures that state actions do not operate in a legal vacuum and that citizens can reasonably foresee the circumstances under which their data must be accessed.

(b) Principle of Necessity

Surveillance or data collection must be strictly necessary to achieve a legitimate aim, such as protecting

national security or preventing serious crime The measure must be the least intrusive means available to achieve the intended objective.

(c) Principle of Proportionality

Even when a surveillance measure pursues a legitimate aim, it must be proportionate to the gravity of the threat. The proportionality test involves:

1. A rational connection between the measure and the objective.
2. Minimal impairment of the right
3. A balancing of the benefit to national security against the harm to individual privacy.

The Puttuswamy judgement in India and the Carpenter ruling in the United States both reaffirm this proportionality standard as essential to any lawful privacy limitation.

1.3 Oversight and accountability mechanism

Effective mechanism of privacy requires not only substantive principles but also procedural guarantees such as:

1. Prior judicial Authorizations: Surveillance should be subject to judicial warrants based on reasonable suspicion.
2. Independent oversight bodies: Institutions like the investigatory powers commissioner's office or the privacy and civil liberties oversight Board ensure compliance.

2. PROPOSALS FOR CHANGE

2.1 Introduction

Balancing the right to privacy with the imperative of national security is a continuous legal and policy challenge. Although existing frameworks in India, the United States, and the United Kingdom, incorporate safeguards such as necessity, legality and proportionality.

The following proposals aim to strengthen the legal architecture governing digital surveillance, data protection, and oversight in order to achieve a more sustainable balance between individual rights and collective security.

2.2 Institutional and oversight reforms

(a) Strengthen judicial Supervision

It must be the primary safeguard against the misuse of surveillance powers:

1. Surveillance warrants should require identifying the subject, scope and duration.
2. Emergency authorizations should be approved by courts within a fixed time frame.
3. Judges should receive technical training to understand complex digital interception.

(b) Promote Transparency and public reporting

Government should issue annual transparency reports disclosing:

1. Number of surveillance warrants issued.
2. Types of data accessed
3. Compliance with privacy protection requirements

Transparency fosters public trust without compromising operational secrecy.

2.3 Technological and procedural safeguards

(a) Privacy by design in state technologies

All government data systems, especially biometric and surveillance databases, should integrate privacy by

design principles, including:

- Data minimization
- Encryption and secure storage
- Anonymization of sensitive data
- Limited retention periods

(b) Use of privacy – Enhancing Technologies

Agencies should invest in privacy- preserving technologies such as:

- Secure multi-party computation for intelligence sharing
- Blockchain based audit trails to ensure accountability for data access

(c) Public awareness and digital literacy

Public awareness campaigns should inform citizens about their privacy rights, available remedies, and responsible use of digital tools.

2.4 Balancing democratic Governance and Security

The ultimate goal is not to choose between liberty and security but to institutionalize a framework that makes them mutually reinforcing.

Security without liberty leads to authoritarianism, while liberty without security leads to instability.

3. Case studies and illustrative conflicts

• India- Aadhaar and state Surveillance

The Aadhaar program, designed for welfare delivery, sparked debate over government access to citizens biometric data. In *Justice K.S Puttswamy V. Union of India* (2017), the supreme court upheld that right to privacy and required the Aadhaar scheme to meet the tests of legality, necessity, proportionality. Concerns remain about data misuse and inadequate safeguards.

• United states -NSA Surveillance and the Snowden Revelations (2013)

Edward Snowdens disclosures exposed the National security Agency's mass surveillance programs that collected global internet and phone metadata. The revelations showed that surveillance often exceeded authorized limits, leading to domestic reforms such as the USA Freedom Act (2015), which curtailed bulk data collection and strengthened oversight.

- **United states- Carpenter v. United states**, the supreme court ruled that accessing historical cell – site location information without a warrant violates the fourth amendment. The decision recognized that digital data revealing detailed personal movements requires privacy protection, even in national security investigations.

CONCLUSION

Balancing privacy and national security in the digital era is an evolving challenge. Comparative jurisprudence shows that legality, necessity, and proportionality remain central to protecting rights while addressing security threats.

References

1. Supreme Court of India, *Justice K.S. Puttswamy (Retd.) v. Union of India* (2017).
2. Supreme Court of the United States, *Carpenter v. United States* (2018).

3. UK Parliament, Investigatory Powers Act 2016.
4. <https://tilburglawreview.com/articles/10.1163/22112596-02001004>
5. <https://quadrangle.michigan.law.umich.edu/index.php/issues/fall-2016/tension>
6. <https://www.ijfmr.com/papers/2025/2/40059.pdf>
7. https://www.researchgate.net/publication/378717983_Balancing_the_Right_to_Privacy_and_National_Security_Interests_in_the_Digital_Age