AL-JAMEI Research Journal
ISSN (Print) 3006-4775 (Online) 3006-4783

https://aljamei.com/index.php/ajrj

Digital privacy vs. National security in the US and EU: Constitutional Boundaries in the surveillance Era

Awais Raza
Department of Law, Dadabhoy Institute of Higher Education, Pakistan
razaawais334@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)

Aliya Saeed
PhD Fellow at School of Law, University of Karachi, Pakistan
(aaliasaeed@yahoo.com)

The manuscript has not been previously published elsewhere and is not being considered by any other journal. The authors read and approved the final version of the respective manuscript.

Note: The authors have no conflict of interest to declare

Abstract

The privacy and security of information on the internet has become a significant constitutional question in the era of surveillance. With governments engaging more and more in surveillance in the fight against terrorism and crime, governments have to strike a fine line between national security and the most important fundamental right to privacy. This paper looks at the constitutional limits within which this balance exists and looks into the legal systems in the U.S. and across the world. It considers the importance of the law on privacy, judicial control, and the consequences of surveillance on the freedom of individuals. Using case studies of countries that have been experiencing such problems, the paper will evaluate the extent to which digital privacy rights are being enforced or infringed in the name of national security. The paper then attempts to give a recommendation on how to better handle this tension in contemporary governance in a more accountable and moral way.

Keywords*: constitutional law, digital privacy, human rights, national security, surveillance*

Introduction

The clash of digital privacy and national security is particularly sharp in the era of surveillance, when we can be more accurate and track data than before, thanks to technology (Slobogin & Brayne, 2023).This fight is contrary to individual constitutional rights to privacy, and the state must guarantee the safety of the world, which is constantly justified by the necessity to counter-terrorism and decrease crime (Fabbrini, 2015). As the world grows more and more growing, the technology of surveillance such as metadata analysis and algorithmic tracking raises even more profound ethical and legal issues regarding the boundaries of state power (Konigs, 2022) Constitutional regimes in the world and the ones that value due process and proportionality are under constant scrutiny as surveillance becomes one of the most serious dangers to the line between a reasonable security operation and voyeuristic intrusion (Donohue, 2023).

Digital privacy is provided by the stipulations of different international and national documents, supporting personal autonomy and avoiding arbitrary interventions of the state in the digital sphere, but often it collides with the requirements of national security in the digital sphere (Wheatley, 2024). The governments justify the need to monitor bulk data to be able to prevent the threat in advance, and critics emphasize that in this way, people lose trust, and the possibility of abuse of the practice without proper controls increases (Kukava, 2023). This balancing process is facilitated by fast technological change; the organizational and societal issues intertwine with legal standards (Dalal et al., 2024). The lack of proper regulatory frameworks in most jurisdictions, including upcoming digital economies, contributes to vulnerabilities, and security interests are superior to privacy protections (Jawaid, 2020).

Finally, constitutional boundaries need to be drawn by resolving these conflicting interests based on the ideas of necessity, proportionality, and judicial discretion (Vargiolu, 2022). With the development of surveillance technologies, the ethical legitimacy of such

surveillance depends on open governance that would not interfere with freedoms at the expense of safety (Mohan, 2025; Nishnianidze, 2024). Resolving this dilemma is important in maintaining democratic principles in the digital era.

Research Justification

This balance between digital privacy and national security is particularly relevant in an age of pervasive technological surveillance. If governments are constantly eavesdropping on citizens in the name of national security, then the right to privacy is sliding at a rapid rate. The motives for surveillance, most of which are usually based on the need to prevent terrorism and the threat of cyber-attack, raise serious constitutional questions about what the state can do and the protection of individual rights. The legal dividing line between these two competing interests is critical in providing a crystal clear understanding of how national security operations can be performed without breaching the fundamental rights of a citizen.

This domain should be researched so it may inform policy and legal decision-making on digital privacy laws. Since the surveillance technology keeps on advancing, the balance between national security concerns and privacy must be reexamined on a regular basis. This study will add to the current debate concerning the best way to balance these interests and what protection needs to be in the constitution to protect privacy without putting national security at risk.

Research Objectives

1. To discuss the historical context of digital privacy vs. national security in the US and EU with respect to constitutional boundaries in the surveillance era.
2. To highlight the theoretical context of digital privacy vs. national security with respect to constitutional boundaries in the surveillance era.
3. To analyze the US and EU laws regarding digital privacy vs. national security with respect to constitutional boundaries in the surveillance era.
4. To identify the key challenges regarding digital privacy vs. national security in the US and EU with respect to constitutional boundaries in the surveillance era.
5. To explore the opportunities for digital privacy vs. national security in the US and EU with respect to constitutional boundaries in the surveillance era.
6. To propose effective prevention and intervention strategies

Research Methodology

This study employed a systematic review methodology, with research objectives established accordingly. A comprehensive literature review was conducted (Komba & Lwoga, 2020). Research findings were categorized based on their content (Hiver et al., 2021; Petticrew & Roberts, 2006), and classified information was incorporated into the study by organizing it into headings (Gan et al., 2021; Pawson et al., 2005). The evaluation of classified information and titles formed the basis of the study (Page, 2021; Rahi, 2017), ensuring the integrity of the research subject and its contents (Egger et al., 2022; Victor, 2008). The criteria for selection are listed.

1. **Relevance:** Researches that directly addressed the questions posed by this study are included.
2. **Quality:** Studies that meet a certain quality threshold (e.g., methodological rigour, bias risk) are included. Most of the research is from Scopus-indexed and Clarivate Analytics journals and reputed publishers.

3. **Recency:** Consideration of the publication date to ensure that the review reflects the most current evidence. Most of the studies are from the last three years.
4. **Language:** Only studies published in English are included.
5. **Data Completeness:** Previous studies must provide sufficient data on outcomes of interest for practical synthesis; this is also ensured in this research.

This study did not use primary data from human participants; therefore, no ethics clearance letter from the ethics committee was required.

Literature Review

The relationship between digital privacy and national security in the surveillance era has received a lot of scholarly attention, and it has been centered on the decrease in constitutional guarantees in light of increasing state surveillance potential (Donohue, 2023). The available literature highlights the problematic essence of such technologies as mass data collection and AI-based surveillance, which often present a security argument over human rights (Wheatley, 2024). This literature demonstrates the legitimacy crisis of government surveillance, in which powers are not limited, which leads to the loss of trust and democratic responsibility among people (Slobogin & Brayne, 2023). Additionally, research has added the necessity of the existence of ethical frameworks that could regulate digital intrusions because, unless proportionality is established, it is then suggested by research that surveillance may drift towards authoritarianism (Konigs, 2022).

Numerous sources are examining the constitutional hypocrisy of the necessity to balance privacy and security requests, particularly following the 9/11 events, when emergency doctrines allow extensive action (Fabbrini, 2015). Researchers criticize the weakness of the current juridical protection, claiming that bulk surveillance usually circumvents judicial control and ignores the necessity principles (Kukava, 2023). Organizational practices enhance such concerns in cyberspace, with the collaboration between the states and the private bodies in information sharing, disrupting the line of public-privacy (Dalal et al., 2024). Reformative regulatory models that seek to incorporate human rights standards in surveillance policies are demanded in this literature (Vargiolu, 2022).

The discourse is also supplemented by regional and global approaches, which depict different ways of solving privacy and security in the digital regulation (Jawaid, 2020). Recent studies consider the effects of Internet governance on this balance that international norms should reduce excessive state powers (Nishnianidze, 2024). More recent cases emphasize new legal approaches to protecting privacy and ensuring the safety of the population (Mohan, 2025). Generally, the body of literature shows that there are still gaps in the implementation of the constitutions, and they should be addressed through multidimensional reforms as a way of successfully going through the ordeal of surveillance.

Historical Context of Digital Privacy and National Security in the US and EU

The history of digital privacy versus national security can be traced back to the mid-20th century, when the first computing and telecommunications developments initiated the first surveillance programs by governments (Donohue, 2023). The U.S. ECHELON system in the post-World War II era represented world signals' intelligence, which served as the precursors of interception of large volumes of data that still informs contemporary models (Fabbrini, 2015). Simultaneously, constitutional privacy rights were introduced with the help of such landmark cases as Olmstead v. Overruled (1928), which raised the point of changing judicial understandings of technological intrusion (Slobogin & Brayne, 2023).These advancements incorporated some of the ground-up tensions between individual protection and state security requirements in the analog-to-digital shift (Konigs, 2022).

The period after 9/11 witnessed a crucial heightening, and acts such as the USA PATRIOT Act extended surveillance authority and supported massive metadata surveillance due to the national security requirements (Jawaid, 2020). In 2013, it was revealed by Edward Snowden that programs like PRISM were in place to demonstrate that the world had eroded privacy, and it has sparked debates that have led to reforms like the USA Freedom Act (Kukava, 2023). It was emphasized in Europe as the Directive on Data Retention was voided as a result of the constitutional restrictions on blanket surveillance (Dalal et al., 2024). It was the time that solidified the era of surveillance as fast digitization increased the tensions between the policies of security and privacy protection (Wheatley, 2024).

Theoretical Context of Digital Privacy and National Security

According to this theory, the right to privacy must be regarded as primary, and any form of invasion of such rights must be supported by principles that do not prejudice the rest. When it comes to surveillance programs, the Rawlsian principles dictate that any encroachment into personal privacy is necessary, proportionate, and subject to examination to determine that it is a legitimate public interest. Deontological ethics and the contributions by Immanuel Kant, specifically, also play an important role in the debate about privacy and security. Kantian ethics focus on the inherent worth of people and the moral imperative to treat people as ends, not as a means to an end. Deontological ethics in the case of surveillance would state that privacy rights cannot be violated in the name of security unless there is a strong moral ground to do so. The privacy right should therefore be upheld at all costs, since it is a part of human dignity.

Utilitarianism, on the other hand, is a theory proposed by philosophers such as Jeremy Bentham and John Stuart Mill. Utilitarianism aims at ensuring that the greatest good is achieved in the greatest number and, in certain instances, may be used to justify surveillance as long as it is a means of national security. According to this viewpoint, the rights to individual privacy can be infringed under the condition that surveillance will lessen the threat of damage to society significantly, e.g., by averting terrorist attacks or cyber threats. The conflict between the values of deontological principles of duty and utilitarian concerns of outcome creates a multidimensional ethical issue in the information age, as national security issues frequently conflict with privacy rights.

Laws Regarding Digital Privacy and National Security in the US and EU

1. **Fourth Amendment of the U.S. Constitution:** The Fourth Amendment guarantees citizens against unreasonable searches and seizures, which is the basis of the right to privacy in America. But the alteration in technology has stretched the boundaries of this constitutional protection.
2. **Electronic Communications Privacy Act (ECPA) 1986:** ECPA law was enacted to control electronic communications, including emails and telephone conversations. Although it was quite revolutionary at the time, it is also widely criticized as failing to consider the reality of contemporary digital surveillance and data storage in full.
3. **Foreign Intelligence Surveillance Act (FISA) 1978:** The act that initially was passed to counter foreign intelligence operations, FISA, gives the government the power to monitor electronic communications. Its provisions have, over the years, been extended, creating fears of domestic surveillance.
4. **USA PATRIOT Act 2001:** The USA PATRIOT Act was passed following the 9/11 attacks, and its provisions extended the capabilities of the government under FISA and

ECPA, which authorized widespread data gathering and computer surveillance in the name of national security.

5. **General Data Protection Regulation (GDPR) 2018:** GDPR is a set of strict regulations on data collection, processing, and sharing in the European Union. It considers privacy as a human right and grants users robust rights over their personal information as a worldwide template of online privacy.

Challenges and Opportunities for Digital Privacy in the Surveillance Era for the US and EU

1. **Surveillance by the Government:** When governments increase surveillance, they are likely to collect too much data in the fight against terrorism and cybercrime. Without the right consent, intelligence agencies can tap into the personal information at the expense of the citizens ' privacy.
2. **Deficiency of Oversight and Accountability:** A lot of surveillance activities have weak external checks, and this gives the agencies the room to carry out their activities in secrecy. This lack of a reviewing body leaves space for misuse and abuse of the data gathered.
3. **Abuse of New Technologies:** Facial recognition, metadata analysis, and artificial intelligence will allow monitoring people at a large scale. In as much as the tools are convenient in security, they can be abused by unnecessarily tracking and focusing on certain groups.
4. **Implications for Constitutional Privacy Rights:** In democratic nations, privacy is a critical right. The issue of increasing surveillance powers usually clashes with constitutional rights and poses legal and moral challenges.
5. **Data Breaches and unauthorized access:** The government and corporate systems have weak security systems that expose sensitive data to hackers. Frauds steal personal data and bring the threat of identity theft and exploitation.
6. **Obsolete and inadequate Privacy legislation:** The current legislation does not match the pace of the swift technological progress. Existing laws and policies are not usually strong enough to deal with the arising risks of online monitoring and information gathering..

Discussion

The current issue of digital privacy versus national security highlights how hard it would be to strike a balance between constitutional rights and the requirements of a secure society. There is justification for surveillance practices on grounds of national security, but the practices pose important ethical and legal issues regarding the contraction of privacy rights. The governments claim that digital surveillance devices are crucial in ensuring that citizens are secure against terrorism and computer attacks. Nonetheless, these actions tend to violate the constitutional right of people to privacy, which is guaranteed by most democratic constitutions. These two interests are not easily reconciled and demand special attention to both precedents of the law and possible impact on civil liberties. Courts' decisions, e.g., Carpenter v. United States (2018), raise the alarm of the increasing issue of government overreach in digital surveillance. The real dilemma, however, is to mandate this through an effective framework that supports privacy rights and provides national security, without interfering with fundamental freedoms.

Conclusion

Large-scale surveillance is a reality that is regularly pushing the constitutional limits of privacy and security in the digital realm. As the level of technological growth significantly develops, a dualistic relationship between national security and individual rights to privacy has to be circumvented by governments. This balance is very difficult to maintain, and constant legal, ethical, and political concerns have to be made as new surveillance technologies and ways of data gathering are being discovered. Through some critical analysis of the available frameworks, one can come up with better safeguards to the privacy aspect, and at the same time ensure that security solutions are not compromised. This constant conversation is needed to support principles of democracy in the digital era.

Recommendations

1. Change laws to consider new forms of surveillance like artificial intelligence, biometrics, and data gathering using digital technologies, and bring them in line with the constitutional provisions on privacy. Conduct campaigns to sensitize people that they have a right to their privacy and the way to ensure that their online data remains unspied by any source, thus avoiding breaches of data security.
2. Establish global digital privacy policies and models that do not violate human rights. Establish international norms to secure people and their data privacy and security, and make countries cooperate on the protection of vital rights. Ensure frequent judicial scrutiny of government surveillance initiatives to be certain that they are executed within the constitutional shields and human rights, so that there is an adequate equilibrium between security and privacy.
3. Embark on effective exercise of checks and balances on the practices of intelligence-sharing. Enhance the oversight and transparency of the surveillance programs to be accountable. Enforce better sanctions for illegal surveillance and breaches of data. Enact stricter punishment for illegitimate surveillance and violations of data protection regulations to dishearten the abuse of authority and failure.
4. Have free oversight institutions where surveillance is conducted on a regular basis and give reports to the community to ensure transparency.
5. Increase privacy by revising the legislation.
6. Limit government surveillance by creating clear, precise boundaries of monitoring where data are gathered, within reasonable and relevant parameters of government threat to national security.
7. Make government surveillance capabilities well-defined.
8. Promote the morality of technological firms dealing with surveillance. Publicize industry ethical principles of tech companies working with data, agreeing that their activities are not just aimed at raising money but at complying with the rights of privacy as well. Promote the judiciary to oversee surveillance programs.
9. Revise judicial understandings of the constitution to be applied to the challenges of the modern age, technology.
10. Sensitise the community on the right to digital privacy.

Research Limitations

There are a number of limitations to this study on the topic of digital privacy and national security. To start with, the use of digital technologies and surveillance techniques is changing at a high pace, and it is hard to analyze the trends that are constantly updated. Facial recognition, artificial intelligence, and the mass data collection system are only being

redefined with new technologies, which can make the research inaccurate due to the latest technologies rapidly setting the trends in privacy and security. Second, the privacy and security laws used by different jurisdictions tend to be complicated, so it may be difficult to provide a universal analysis. Research is also limited to the data on governmental surveillance programs, which are available and accessible since a lot of the programs are either classified or not easily accessible. Lastly, the socio-political aspects like the political favoritism, the issue of national security, and the differing views of people against privacy complicate the objective examination further. Such restrictions have to be considered during the interpretation of the results of this study.

Research Implications

This research has far-reaching implications for policymakers as well as the legal fraternity. This paper has identified a necessity to have more cohesive and sound models to find a balance between privacy and national security considerations. The outcomes of this study can be used in future laws, especially regarding strengthening the privacy of citizens against increasing surveillance. In addition, it also demands the creation of even tougher supervisory mechanisms and the enforcement of even stricter transparency standards in the sphere of government surveillance practices.

Moreover, this study may be of use when designing the discourse on the ethical aspects of the digital era surveillance. The study suggests increased human security measures by being more human-focused and highlighting constitutional safeguards and human rights. Policymakers and legislators can use the research to develop a better idea of how the current legal protection can be modified to accommodate the current concerns of surveillance, while keeping the basic freedoms intact without prejudice to national security.

Future Research Directions

Future studies on digital privacy and national security ought to consider a few essential areas to resolve the already present challenges. To begin with, a better exploration of existing surveillance oversight processes may identify the accountability and transparency loopholes. Also, discussing international case studies in the field where privacy regulations and surveillance practices have proved to strike a balance would be interesting to learn about best practices. The ethical issue that the future research might focus on is also the investigation of emerging technologies of surveillance, including AI-based monitoring systems or biometric data collection, since they present a new threat to privacy.

It is also important that the question of the changing nature of the relationship between international cybersecurity threats and national surveillance policies should also be the subject of research, especially how international treaties or antagonisms affect the national legislation on privacy. In addition, research into the role of socio-political influences in the formation of surveillance policy would provide a more effective explanation of the role of the public in determining such constitutional controversies. The areas will keep on being critical as governments and people deal with the age of digital surveillance.

References

Dalal, R.S., Bennett, R. & Posey, C. (2024). Security, privacy, and surveillance in cyberspace: Organizational science concerns and contributions. Journal of Business and Psychology, 39(2), 1023–1026. https://doi.org/10.1007/s10869-024-09968-1

Donohue, L. K. (2023). Surveillance, state secrets, and the future of constitutional rights. The Supreme Court Review, 2022, 351–436. https://doi.org/10.1086/724432

Egger, M., Higgins, J. P., & Smith, G. D. (Eds.). (2022). Systematic reviews in health research: Meta-analysis in context. John Wiley & Sons.

Fabbrini, F. (2015). Introduction: Privacy and national security in the digital age. In the Research Handbook on Human Rights and Digital Technology (pp. 1–14). Edward Elgar Publishing. https://doi.org/10.1163/22112596-02001004

Gan, J., Xie, L., Peng, G., Xie, J., Chen, Y., & Yu, Q. (2021). Systematic review on modification methods of dietary fiber. Food Hydrocolloids, 119, Article 106872. https://doi.org/10.1016/j.foodhyd.2021.106872

Hiver, P., Al-Hoorie, A. H., Vitta, J. P., & Wu, J. (2021). Engagement in language learning: A systematic review of 20 years of research methods and definitions. Language Teaching Research. Advance online publication. https://doi.org/10.1177/13621688211001289

Jawaid, T. (2020). Privacy vs national security. International Journal of Computer Trends and Technology, 68(7), 1–7. https://doi.org/10.14445/22312803/IJCTT-V68I7P101

Komba, M. M., & Lwoga, E. T. (2020). Systematic review as a research method in library and information science. In P. Ngulube (Ed.), Handbook of research on connecting research methods for information science research (pp. 80–94). IGI Global. https://doi.org/10.4018/978-1-7998-1471-9.ch005

Konigs, P. (2022). Government surveillance, privacy, and legitimacy. Philosophy & Technology, 35(1), Article 19. https://doi.org/10.1007/s13347-022-00503-9

Kukava, K. (2023). Balancing the right to privacy and national security interests in the digital age. Journal of Law, 2, 338–353. https://doi.org/10.60131/jlaw.2.2023.7711

Mohan, C. (2025). Surveillance and national security: Balancing privacy and public interest for a safer society. In Proceedings of the National Seminar on Enhancing Privacy Protection in the Digital Age: Legal Challenges & Innovations (NSEPPDA 2025) (pp. 537–561). Atlantis Press. https://doi.org/10.2991/978-2-38476-426-6_26

Nishnianidze, A. (2024). Surveillance in the digital age. European Scientific Journal, 20(37), 1–24. https://doi.org/10.19044/esj.2024.v20n37p1

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., & Moher, D. (2021). Updating guidance for reporting systematic reviews: Development of the PRISMA 2020 statement. Journal of Clinical Epidemiology, 134, 103–112. https://doi.org/10.1016/j.jclinepi.2021.02.003

Pawson, R., Greenhalgh, T., Harvey, G., & Walshe, K. (2005). Realist review—A new method of systematic review designed for complex policy interventions. Journal of Health Services Research & Policy, 10(1), 21–34. https://doi.org/10.1258/1355819054308530

Petticrew, M., & Roberts, H. (2006). Systematic reviews in the social sciences: A practical guide. Blackwell Publishing. https://doi.org/10.1002/9780470754887

Rahi, S. (2017). Research design and methods: A systematic review of research, sampling issues, and instruments development. International Journal of Economics & Management Sciences, 6(2), Article 403. https://doi.org/10.4172/2162-6359.1000403

Slobogin, C., & Brayne, S. (2023). Surveillance technologies and constitutional law. Annual Review of Criminology, 6, 219–240. https://doi.org/10.1146/annurev-criminol-030421-035102

Vargiolu, A. (2022). Personal privacy and Internet regulation: Balancing security and freedom in the digital age. https://doi.org/10.13140/RG.2.2.23935.21920

Victor, L. (2008). Systematic reviewing in the social sciences: Outcomes and explanation. Enquire, 1(1), 32–46. https://www.nottingham.ac.uk/sociology/documents/enquire/volume-1-issue-1-victor.pdf

Wheatley, M. C. (2024). Ethics of surveillance technologies: Balancing privacy and security in a digital age. Premier Journal of Data Science, 1, Article 100001. https://doi.org/10.70389/PJDS.100001