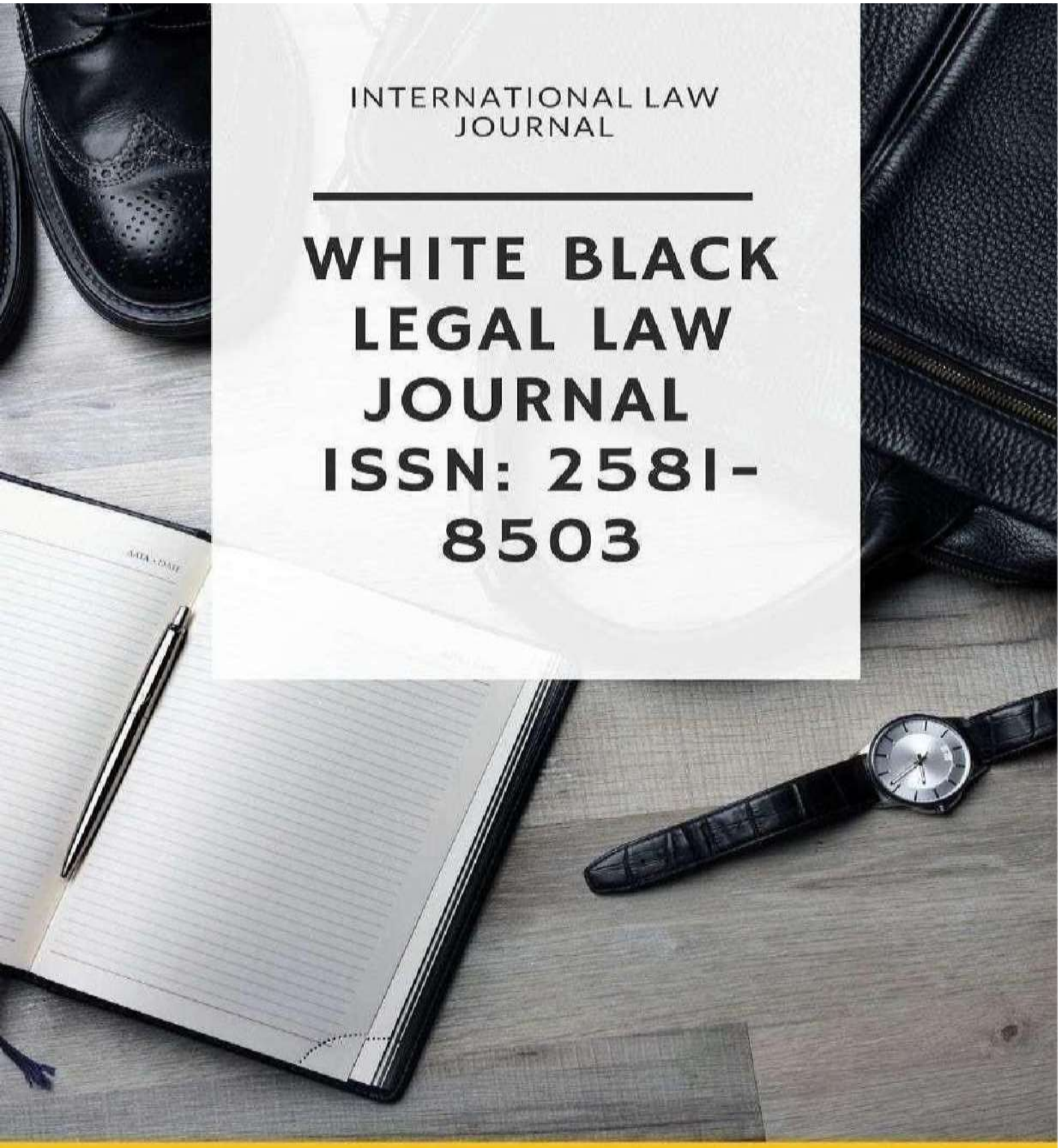

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in ‘Intercountry adoption laws from Uttranchal University, Dehradun’ and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

www.whiteblacklegal.co.in
Volume 3 Issue 1 | April 2025 ISSN: 2581-8503

SURVEILLANCE, DATA PRIVACY, AND DEMOCRACY: A COMPARATIVE STUDY OF NATIONAL SECURITY POLICIES

AUTHORED BY - DR. SM. AZIZUNNISAA BEGUM & B. SANTOSH KUMAR

I. INTRODUCTION

The rise of digital technologies has fundamentally transformed the nature of surveillance creating complex challenges for national security, data privacy, and democracy.[1] One of the most prominent examples of this shift occurred in March 2018, when Cambridge Analytical was exposed for illegally harvesting data from more than 50 million Facebook profiles.[2] This data was used to create psychological profits of users, which in turn influenced the results displayed in their news feeds.[3] The scandal revealed the significant role that data manipulation and surveillance play in modern political processes, especially during elections, as seen in the 2016 U.S. presidential campaign. Facebook's involvement, through the data-sharing activities of Aleksandr Kogan's app[4], highlighted the blurred lines between social media platform, data privacy, and political influence.[5]

Cambridge Analytical is the growing nexus between politics, surveillance, and technology.[6] It also added to the global concern around the personal data safety, sharing of data and broader democratic governance implication. The mass surveillance of millions of users in the digital

[1]Unver, H.Akm. *Politics of Digital Surveillance, National Security and Privacy.* Centre for Economic and Foreign Policy Studies, 2018. *JSTOR,* https://www.jstor.org/stable/resrep17009 Accessed 15 October 2024.
[2]Patel, N., Arora, V., Sekhar, M.S., De, T., Gupta, C.A.R., Penny, N., Saraf, A. and Allegations, 'CBI files case against Cambridge Analytica for illegal harvesting of Facebook users data in India' *The Economic Times*https://economictimes.indiatimes.com/news/politics-and-nation/cbi-files-case-against-cambridge-analytica-for-illegal-harvesting-of-facebook-users-data-in-india/articleshow/80400033.cms?from=mdr accessed 15 October 2024.
[3]Lien Faelens and others, The relationship between Instagram use and indicators of mental health: A systematic review' (2021) 4 *Computers in Human Behavior Reports* 100121 https://doi.org/10.1016/j.chbr.2021.100121 accessed 16 October 2024
[4]Dan Sabbagh, 'Revealed: Aleksandr Kogan Collected Facebook Users' Direct Messages' (The Guardian, 13 April 2018) https://www.theguardian.com/uk-news/2018/apr/13/revealed-aleksandr-kogan-collected-facebook-users-direct-messages accessed 16 October 2024
[5]University of New South Wales Canberra, Defence Research Institute, *Understanding Mass Influence: A Case Study of Cambridge Analytica* (UNSW, 2023) https://www.unsw.edu.au/content/dam/pdfs/unsw-adobe-websites/canberra/research/defence-research-institute/2023-02-Understanding-Mass-Influence---A-case-study-of-Cambridge-Analytica.pdf accessed 18 October 2024
[6]Bipartisan Policy Center, 'The Cambridge Analytica Controversy' (Bipartisan Policy Center, 28 March 2018) https://bipartisanpolicy.org/blog/cambridge-analytica-controversy/ accessed 14 October 2024.

era is an ethical and legal challenge, but the unauthorised access to millions of user's data without their consent and ability to manipulative public opinion through psychological profiling, exemplifies it.[7]

The argument around the notion of digital surveillance, which is characterized by the collection, recording, and processing of a person's online activities in real time or in the past without that person.[8] By contrast, privacy is understood to be something to do with the right to be free from unauthorised intrusion. While these aren't new ideas, the rapid growth of social media and the technology of digital connectivity has pushed the line of the surveillance debate farther.[9]

The Surveillance theory has roots in Jeremy Bentham's idea of the 'panopticon' and Michel Foucault's panopticon."[10]These frameworks carve out a system of and control which individual is constantly monitored and not even knowing whether one is being observed. The government, businesses, and private citizens have implemented surveillance techniques that are as wide and as complicated as the panopticon, given today's digital environment. First, come the ramifications for democracy, civil liberties and individual freedoms that are inevitable as we move further along into the digital era, and raise immediate question of the balance to be struck between securities with privacy rights in today's society.

1. Statement of Problem:

Tension exists between data privacy and practices of monitoring in democratic governance. Unlikely to be compatible with civil rights and diminishes individual privacy increases surveillance often in the name of national security. The balance that we ask comes from democratic national states because this is an essential thing. How do we legitimately maintain surveillance in a way that is an essential thing? How can we properly continue surveillance without going too far in term of transparency, protecting fundamental rights, and conducting surveillance?

[7]Sangeeta Mahapatra, *German Institute for Global and Area Studies* (GIGA) *available at*: https://www.giga-hamburg.de/en/the-giga/team/mahapatra-sangeeta accessed 26 October 2024
[8] H. Akm , Unver *Politics of Digital Surveillance, National Security and Privacy*. Centre for Economic and Foreign Policy Studies, 2018. JSTOR, https://www.jstor.org/stable/resrep17009 Accessed 15 October 2024.
[9]Office of the United Nations High Commissioner for Human Rights, 'The Right to Privacy in the Digital Age' (OHCHR, 2013) https://www.ohchr.org/en/stories/2013/10/right-privacy-digital-age accessed 16 October 2024.
[10]The Guardian, 'Panopticon: The Lasting Impact of Bentham's Radical Prison Concept on Digital Surveillance' (23 July 2015) https://www.theguardian.com/technology/2015/jul/23/panopticon-digital-surveillance-jeremy-bentham accessed 14 October 2024.

2. Objective:

Considering the tension between data privacy and monitoring practices and democratic governance, how increased monitoring though seemingly well-displaced by national security's needs can undermined civil rights and individual privacy exacerbates needs to be explored. The objective of this is to discover how democratic nations might manage continuing to be transparent in surveillance practices and prevent government expansion, even as they safeguard vital rights through balancing security and privacy.

3. Scope:

This paper explores Chinese, US, and European Union national security regulation of data privacy and surveillance. It looks at China's authoritarian surveillance system, EU's data protection framework such as the GDPR, and widespread monitoring practices in the United State. The focus of this study is that each region balances the need of individual rights and security.

4. Research Question:

1. Why do different countries prioritize surveillance over data privacy in their national security policies?
2. How do national security policies in various countries balance the need for surveillance with the protection of individual data privacy rights?
3. Why do citizens in some democracies accept higher levels of surveillance compared to others, despite concerns over privacy?
4. How do national security policies in various countries balance the need for surveillance with the protection of individual data privacy rights?

II. HISTORICAL CONTEXT OF SURVEILLANCE AND DEMOCRACY

Surveillance has been one of the means used by governments to achieve a motive-to achieve control. Once war breaks out, or there is civil unrest. The surveillance ball gets rolling in order to keep everyone within the fold. Through most of World War I and World War II, major nations established extensive systems to surveil dissenting voices[11] and suppress or deter

[11]S Basu and S Sen, 'Silenced Voices: Unravelling India's Dissent Crisis Through Historical and Contemporary Analysis of Free Speech and Suppression' (2023) 33(1) Information & Communications Technology Law 42 https://doi.org/10.1080/13600834.2023.2249780Accessed on 16 October 2024 .

espionage.[12] The process was framed as a matter of national security. Further, that set a precedent for subsequent surveillance efforts while exposing a tension between government oversight and private liberty.[13]

In democratic setting, there can be a proper balance between surveillance and behaviour code, such as freedom of speech, privacy, and civil liberties. Existence of surveillance practices raises the possibility of self-censorship by making citizens fear constantly surveillance. That threatens as open democratic discourse.[14]

The events of 9/11 resulted in a significant increase in surveillance measures, under the protection of national security. Authorities were granted additional authority under the new law. USA PATRIOT ACT to surveil communications on a scale never seen before.[15] The NASE, on the other hand, the PRISM program permitted the gathering of personal information on Individual in the widest possible scope without restrictions. Any type of authorization.[16] Likewise, although their purpose is to prevent acts of terrorism, they also have other effects. Sparked an ongoing discussion on the conflict between national security. Privacy rights for individuals, as well as civil liberties within democratic societies.

III. COMPARATIVE ANALYSIS: NATIONAL SECURITIES POLICIES

1. First Case Study: United States

After the 9/11 attacks, the USA PATRIOT ACT and the Foreign Intelligence Surveillance Act (FISA) become crucial elements of United States' increased surveillance efforts. The PATRIOT ACT granted the National Security Agency (NSA) the power to monitor communications for counterterrorism objectives through roving wiretaps, bilk data collection, and sneak-and-peek warrants. Sections 702 of the FISA Amendments Act (2008) allowed the surveillance of foreign individual, often accidently capturing the communication of American

[12]Rebecca Sanders, 'Surveillance' in *Plausible Legality: Legal Culture and Political Imperative in the Global War on Terror*, Oxford Studies in Culture and Politics (New York, 2018; online edn, Oxford Academic, 23 Aug. 2018) https://doi.org/10.1093/oso/9780190870553.003.0005 accessed 15October 2024.
[13]Sidharth,'A Study on the Impact of the Juvenile Justice Act on Recidivism Rates' (2024) IJCRT 2405285 https://ijcrt.org/papers/IJCRT2405285.pdf accessed 14 October 2024.
[14]Michaela Padden 'Transformation of Surveillance in Digitalisation Discourse' (2021) *Policy Review*https://policyreview.info/articles/analysis/transformation-of-surveillance-in-digitalisation-discourse accessed 14 October 2024
[15]Deeks, A, "Legal Framework" (2016) https://www.ilsa.org/Jessup/Jessup16/Batch%202/DeeksLegalFramework.pdf accessed 14 October 2024.
[16]Glenn Greenwald & Ewen MacAskill, 'US Tech Giants' Data Used by NSA' (6 June 2013) https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data accessed 18 October 2024.

citizen.[17]

It is widely accepted, since after the 2013 Edward Snowden leaks[18] revealed programs like PRISM and Upstream, gathering large amounts of metadata from millions of people without warrants that the NSA was doing so much. The government was cleverly deceiving itself and the public was outraged to discover the government had violated rights protected by the Fourth Amendment by violating its privacy.

The USA FREEDOM Act of 2015[19] was passed, leading to increased supervision and transparency while restricting the gathering of NSA's mass data. Despite these measures are serious concerns concerning the loss of privacy rights and balance between security and civil liberties remain to be prominent.

These policies have a noteworthy impact on democracy. Decisions made by the courts in the cases, suchin 2015 ruling by the U.S. Court of Appeals have establish positive aspects of the NSA's surveillance programs to be unlawful. Trust in government institution has been weakened due to unlawful, and this trust in government institutions has been weakened ascribed by concerns about widespread surveillance, causing individuals censoring themselves and restrains their free speech. However, surveillance is needed for the national security, further its impact on privacy and democratic values be still a subject of debate.

2. Second Case Study: EU

The General Data Protection Regulation (GDPR), which went into effect in 2018, is the leading cause, of why the European Union (EU) leads the world in data privacy. In addition to, demanding consent for the usage data, GDPR is extremely strict on data integration, processing and storage because people have rights such as the right of be forgotten.

EU member states have difficulties in notable right balance between privacy and national security. In the stellar example of Digital Rights Ireland (2014), European Court of a Justice

[17]American Civil Liberties Union, 'Warrantless Surveillance Under Section 702 of FISA' (American Civil Liberties Union) https://www.aclu.org/issues/national-security/warrantless-surveillance-under-section-702-fisa accessed 14 October 2024.

[18] Ewen Macaskill &Garbriel Dance,'Snowden NSA Files: Surveillance Revelations Decoded' (1 November 2013) https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1 accessed 18 October 2024

[19]USA FREEDOM Act 2015, Public Law No 114-23, 129 Stat 268 (2015).

(ECJ) provides a wholesale prohibition of indiscriminate data retention by rejecting unbridled government monitoring. Yet in response to security risks, France and Germany have taken measures to step up surveillance, often in contravention of GDPR rules.

It also complicates efforts to share intelligence, making it harder for members states to interpret the various data protection regulations in the same way and crating tension between the expectation of individual rights to privacy and the realities of collective security In order to keep its promise of data privacy the EU needs to negotiate its way through these challenges which involve changing national security policies to bring about security issues while other don't..

3. Third Case Study: China

With the use of technologies like the social credit system and the Great Firewall[20], China has one of the most sophisticated surveillance systems in the world. The Great Firewall gives the government the ability to regulate internet access and keep a tight eye on residents' actions by blocking access to foreign websites and politically sensitive information. Established in the mid-2010s, the social credit system evaluates residents according to their adherence to social standards and the law, generating ratings that impact their access to privileges like employment, loans, and travel.

Data privacy is almost non-existent in this situation. The government gathers a lot of personal data from several sources, such as biometric information and internet usage. The state requires data sharing from businesses like Tencent and Alibaba, allowing for widespread monitoring without permission.

There are significant ramifications for people' liberties. A culture of self-censorship is fostered by ongoing monitoring, discouraging political dissent or criticism of the government, which can have serious consequences including detention or loss of employment. As a social control tool, the social credit system discourages nonconformity and strengthens governmental power. In the end, China's monitoring system undermines democratic values by stifling free expression and political engagement while strengthening the regime's hold on power.

[20]Erik Roberts, 'Free Expression vs. Social Cohesion: China's Policy' (Stanford University, 2011) https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreeExpressionVsSocialCohesion/china_policy.html accessed 18October 2024.

IV. IMPACT ON CIVIL LIBERTIES AND DEMOCRATIC INSTITUTIONS

1. The dilemma of privacy against security

Government throughout the world defend mass monitoring as necessary to protect national security. Monitoring is, state officials say, an indispensable tool at a time when organised crime, cyber-crime and terrorism all present serious dangers, and serious threats. For example, the USA PATRIOT Act, which was passedin the post result of the 9/11 attacks, which increased the surveillance powers of the U.S. government and also it enabled organizations such as the NSA to monitor communications on aimmense scale in order to prevent terrorism. Comparably on other hand, in China, the social credit system and the Great Firewall have their defenders describe the two as techniques to enforce social order and combat criminal behaviour, frequently in the name of national security.[21]

Even after these assertions, the trade-off between security and privacy is still a controversial subject. Government often collect huge amount of personal data people but they don't know or agree to it and that's not ok. Edward Snowden's tiresome 2013 leaks to media exposed the truly broad extent of U.S. government surveillance: how organisations like the NSA collected and gathered data on millions of people with little or no legal over sight. Public doubt has risen, however, about whether the aim is to protect national security or, as many suspect, whether it is an unessential invasion of people's privacy. Critics argue that mass monitoring, and often more, often crosses into territory that goes well beyond the actual needs and threatens to undermine sorely needed individual privacy and civil freedom. The problem with these programs is also their lack of openness regarding these initiatives, far too aften people are in the dark about how much of their personal information is being tracked and stored.[22]

2. Chilling Effects on Freedom of Speech

Freedom of expression may be suppressed by surveillance, which is one of the tenets of a functioning free society. They avoid talking about it out of fear of government reprisals when they know that there are individuals keeping an eye out for such divisive or contentious

[21]GIGA Focus, 'Digital Surveillance and the Threat to Civil Liberties in India' (no date) https://www.giga-hamburg.de/en/publications/giga-focus/digital-surveillance-and-the-threat-to-civil-liberties-in-india accessed 4 November 2024.
[22]American Civil Liberties Union, 'Warrantless Surveillance Under Section 702 of FISA' (American Civil Liberties Union) https://www.aclu.org/issues/national-security/warrantless-surveillance-under-section-702-fisa accessed 14 October 2024.

viewpoints. It limits free expression and public discourse, both of which are essential in democracies. In China, where the power of its monitoring apparatus is barely consented, the result is terrifying. Self-censorship is encouraged by the state's social credit system, which punishes behaviour or statements that deviate from accepted norms by placing a person on a blacklist. Chinese individual can maintain their social credit rating by suppressing demonstrations and refraining from discussing delicate political subjects, which is a from of surveillance that can limit free expression.[23]

Surveillance can also hinder the freedom of speech and political activities in democracy. And yet, with their communications being monitored, many Americans expressed their concerns in talking part in political activities or making critical opinion online after hearing the revelation of NSA. Much like this, many of those in Europe have admitted they have gove out of their ways to alter how they live to ensure they aren't being tracked, not least those living in more data retention friendly nations. The chilling effect, therefore, extends beyond authoritarian government itself because it extends into democracies like ours that respect free expressionbut have difficulty coordinating a response to extensive monitoring.[24]

3. Public Confidence in Democratic Establishments

Mass monitoring greatly affects the public confidence of democratic institutions and the government. Such actions generally come to people as an abuse of government and they start to doubt the sincerity and the intention behind the leaders. Revulsions in the Snowden spilling made people in the United Stated not trust the government agencies these anymore. Many Americans think their constitutional rights are being violated and have been demanding legislation to limit government surveillance capabilities and this is what there have been a lot of requests of something to be done to changing that. Despite laws like the USA FREEDOM Act addressing some of these concerns, the privacy doesn't seem to have been handled at the government level in a way that has inspired public confidence.[25]

---

[23]S Basu and S Sen, 'Silenced Voices: Unravelling India's Dissent Crisis Through Historical and Contemporary Analysis of Free Speech and Suppression' (2023) 33(1) Information & Communications Technology Law 42 https://doi.org/10.1080/13600834.2023.2249780Accessed on 16 October 2024 .

[24]Rebecca Sanders, 'Surveillance' in *Plausible Legality: Legal Culture and Political Imperative in the Global War on Terror*, Oxford Studies in Culture and Politics (New York, 2018; online edn, Oxford Academic, 23 Aug. 2018) https://doi.org/10.1093/oso/9780190870553.003.0005 accessed 15October 2024.

[25]GIGA Focus, 'Digital Surveillance and the Threat to Civil Liberties in India' (no date) https://www.giga-hamburg.de/en/publications/giga-focus/digital-surveillance-and-the-threat-to-civil-liberties-in-india accessed 4 November 2024.

Balancing security and privacy policies is the key for us to retain public trust in the European Union. Under the EU General Data Protection Regulation (GDPR), you want to protect people's private data while allowing for appropriate monitoring of surveillance necessary to prevent national security disasters. However, nations such as France and Germany perennially face the wrath pf public opinion when they seek to extend the scope of the monitoring or data retention laws. A continuous discussion on the suitable scope of government surveillance to counteract the struggle between national security and private rights makes attempts to keep the public trust even harder.

The effect in China is complicated. The state maintains a vast monitoring machinery that encourages some people to cooperate and ally with the state, and other to mistrust even more, especially if someone feels repressed or unfairly singled out. Monitoring pervades throughout its resident; self-confidence is undermined and ultimately leads to a society where governmental control of individual rights is complete.

SURVEILLANCE AND DEMOCRACY: FUTURE TIMELINE

1. Developments in Technology

Surveillance is being makes far-reaching changes in by technological innovations like biometrics, facial recognition, and Artificial Intelligence (AI). Real time scrutiny of massive data sets, potential threat trends and behaviours, are done by the AI. However, artificial intelligence (AI) allows governments to process multiple cameras, or to process digital records in a single go, making it more effective though also more invasive. In nations like China, where facial recognition technology is widely employed for social control and public monitoring, it is possible to identify people in public places, frequently without their agreement.[26]

Biometric data, such as fingerprints or facial recognition, is being more and more included into identity and security systems, and it is a powerful surveillance tool. But they bring privacy concerns. Accuracy and extent of these technologies coupled with potential for ongoing citizen surveillance lend themselves toward government control of people's private lives and

[26]Ramanpreet Kaur, DušanGabrijelčič and TomažKlobučar, 'Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions' (2023) 97 Information Fusion 101804 https://doi.org/10.1016/j.inffus.2023.101804.

activity.[27]

The combination of fingerprints and face scans with biometric information increasingly being used in identity and security systems offers a powerful surveillance tool. There are privacy issues arising from this development, though. More government surveillance over people's lives and activities also including more control over their private lives and it becomes more likely the more precise and extensive these technologies are.[28]

2. **Reforms in the Law**

With the development of surveillance technology, it is necessary to urgently change laws, protecting data privacy. The General Data Protection Regulation (GDPR) in the European Union is one of the strongest privacy regulations, which instructs state as well as other businesses to seek express authorization before collection of personal data/ these rules are meant to balance private security and privacy.

Additionally, there has to be reinforced the procedures of supervision. For this surveillance procedure need to be supervised by impartial organizations to ensure that they are appropriate, lawful. In attaining rebuild public confidence, crucial measures to curb government abuse such as judicial review and openness (announcing and exposing its monitoring by way of public reporting also including the right to contest the monitoring).

3. **Public Activism and Resistance**

Civil society was the only group capable of opposing such a proposal. Group like Privacy International and the Electronic Frontier Foundation (EFF) are advocating for stricter privacy laws, raising public awareness, and contesting overreaching monitoring programs. The misuse of covert monitoring by whistleblowers like Edward Snowden necessitates a global conversation about privacy.

[27]Office of the Victorian Information Commissioner, 'Biometrics and Privacy: Issues and Challenges' (2024) https://ovic.vic.gov.au/privacy/resources-for-organisations/biometrics-and-privacy-issues-and-challenges/ accessed 18October 2024.

[28]Youyang Qu, Mohammad Reza Nosouhi, Lei Cui, and Shui Yu, 'Privacy Preservation in Smart Cities' in *Smart Cities Cybersecurity and Privacy* (2019) 75-88 https://doi.org/10.1016/B978-0-12-815032-0.00006-8 accessed 18 October 2024.

CONCLUSION

To understand the interplay between surveillance and data privacy, as well as between democracy and national security, this research compared the national security policies of the US, EU, and China. U.S. laws like the USA PATRIOT ACT and Snowden revelations place privacy vs security issues in the marketplace, as they play out one over the other. Laws like the GDPR are meant to balance these interests, but member state security coordination feels unbalanced. However, here is a prime example of an authoritarian regime, where there is considerable sacrificing of individual liberties in form of colossal monitoring networks.

Technological developments like artificial intelligence (AI) and biometrics are transforming the surveillance environment, underscoring the necessity of robust legislative changes to safeguard individuals' right to privacy. The growing need for accountability in government activities is evidenced by civil society actions and advancements in privacy-enhancing technology.

Concluding remarks

It is vital to strike a balance among democratic liberties and national security. Legislators should establish responsible, accountable, transparent frameworks which could balance security requisite with privacy protection.

An Appeal for Action

To comprehend the long-term impacts of monitoring on civil freedoms, more study is essential. Public discourse on monitoring methods will enable people to defend their rights and guarantee the preservation of democratic values.

Reference

- American Civil Liberties Union, 'Warrantless Surveillance Under Section 702 of FISA' (American Civil Liberties Union)
- Bipartisan Policy Center, 'The Cambridge Analytica Controversy' (Bipartisan Policy Center)
- Dan Sabbagh, 'Revealed: Aleksandr Kogan Collected Facebook Users' Direct Messages' (The Guardian, 13 April 2018)
- Deeks, A, "Legal Framework" (2016)

- Ewen Macaskill &Garbriel Dance,'Snowden NSA Files: Surveillance Revelations Decoded'
- Glenn Greenwald & Ewen MacAskill, 'US Tech Giants' Data Used by NSA'
- H. Akm , Unver Politics of Digital Surveillance, National Security and Privacy. Centre for Economic and Foreign Policy Studies, 2018. JSTOR
- Lien Faelens and others, The relationship between Instagram use and indicators of mental health: A systematic review' (2021) 4 Computers in Human Behavior Reports 100121
- Michaela Padden 'Transformation of Surveillance in Digitalisation Discourse' (2021) Policy Review
- Office of the United Nations High Commissioner for Human Rights, 'The Right to Privacy in the Digital Age' (OHCHR, 2013)
- Patel, N., Arora, V., Sekhar, M.S., De, T., Gupta, C.A.R., Penny, N., Saraf, A. and Allegations, 'CBI files case against Cambridge Analytica for illegal harvesting of Facebook users data in India' The Economic Times
- Rebecca Sanders, 'Surveillance' in Plausible Legality: Legal Culture and Political Imperative in the Global War on Terror, Oxford Studies in Culture and Politics (New York, 2018; online edn, Oxford Academic, 23 Aug. 2018)
- S Basu and S Sen, 'Silenced Voices: Unravelling India's Dissent Crisis Through Historical and Contemporary Analysis of Free Speech and Suppression' (2023) 33(1) Information & Communications Technology Law 42
- Sangeeta Mahapatra, German Institute for Global and Area Studies (GIGA)
- Sidharth,'A Study on the Impact of the Juvenile Justice Act on Recidivism Rates' (2024) IJCRT 2405285
- The Guardian, 'Panopticon: The Lasting Impact of Bentham's Radical Prison Concept on Digital Surveillance' (23 July 2015)
- University of New South Wales Canberra, Defence Research Institute, Understanding Mass Influence: A Case Study of Cambridge Analytica (UNSW, 2023)
- Unver, H.Akm. Politics of Digital Surveillance, National Security and Privacy. Centre for Economic and Foreign Policy Studies, 2018. JSTOR.