Democracy and Spyware: The Case of India

Ahissa Breanna Rice

Submitted to the faculty of the Virginia Polytechnic Institute and State University in partial fulfillment of the requirements for the degree of Master of Arts In Political Science

Aaron F. Brantly, Chair

Nataliya D. Brantly

Paul C. Avey

21 April 2025

Blacksburg VA

Keywords: Democracy, spyware, digital surveillance, Pegasus, privacy rights, India, European Union, comparative analysis, MSSD

Democracy and Spyware: The Case of India

Ahissa Breanna Rice

ABSTRACT

There is troubling contradiction between India's status as the world's largest democracy, with a constitution that enshrines privacy as a fundamental right, and the government's routine engagement in invasive digital surveillance of its own citizens. The Pegasus spyware revelations exposed how Indian authorities exploit systemic flaws, legal loopholes, and lack of oversight to illegally spy on dissidents, journalists, opposition figures, and activists, disregarding constitutional guarantees. This study uses the Most Similar Systems Design (MSSD) method to compare India's surveillance regime with the European Union's GDPR plus associated frameworks. This comparison aims to find the reasons for differing surveillance practices between the two, despite similar legal and constitutional protections. This analysis will examine five key variables: constitution, laws, policies/regulations, diversity of population, and security.

This analysis focuses on weaknesses in India's laws that enable government overreach, focusing on the insufficient oversight and highlighting the need for reforms to adjust surveillance practices with democratic norms. This study which examines the important discrepancy between India's strong privacy rights as outlined in law and its largely unregulated surveillance powers, highlights the urgent need for thorough reforms. These reforms are necessary to limit surveillance powers, to firmly enshrine due process, and to enable independent oversight. A comparative analysis between India and the EU aims to better understand the reasons and factors leading to the misuse of surveillance powers in India, and to also lead towards potential solutions

to better safeguard citizens' rights in the digital age. This thesis contributes to the ongoing discussion about how democracies manage the challenges caused by these modern surveillance technologies and how democracies do this while still upholding and protecting both the rule of law and individual privacy rights.

Democracy and Spyware: The Case of India

Ahissa Breanna Rice

GENERAL AUDIENCE ABSTRACT

This research paper examines India's status as the world's largest democracy with a constitution that enshrines privacy as a fundamental right that contradicts these terms by use of intrusive surveillance technologies being directed against its own citizens. This study reveals how similar democratic systems have developed drastically different approaches when it comes to surveillance practices through comparative analysis using Mill's Most Similar Systems Design (MSSD) with the European Union. India's usage of Pegasus spyware against journalists, activists, and political dissidents highlights this ongoing issue. This paper identifies specific institutional weaknesses that enable surveillance overreach despite India's constitutional protections by analyzing five key variables: constitution, laws, policy/ regulatory, diversity, and security.

Independent oversight mechanisms and judicial checks on executive power are needed based on the findings showing that constitutional privacy guarantees alone are not sufficient. India and the EU both face many similar security challenges, but their institutions respond in very different ways. The EU requires strict judicial authorization and also tests the proportionality for surveillance, but India allows broad exemptions for government agencies and also minimizes accountability. This research paper contributes to the understanding of how democratic principles can be weakened through institutional choices in the digital age,

highlighting that there is a need for reforms and transparency to protect democratic values in an increasingly digitalized world

Table of Contents

Acknowledgements

I owe my deepest gratitude to Dr. Aaron Brantly, whose exceptional mentorship guided this research journey. His patience and wisdom not only directed my work but also led me to join the Tech4Humanity Lab, where I discovered my true potential as a researcher. Under his leadership, I've encountered countless opportunities I could have never imagined and joined a research community where I could truly thrive and develop my own research passions. His extensive expertise in cybersecurity and willingness to push boundaries have been invaluable throughout my time at Virginia Tech and with the Tech4Humanity Lab.

To my mom and dad, I could not have accomplished any of this without you in my corner. Your unwavering support, late-night pep talks, and steadfast belief in me kept me going through every challenge and obstacle I faced. Your constant love and encouragement have been my foundation, and for that, I am forever grateful.

Chapter 1: Introduction the Case of India

Problem Statement

The Internet is an important part to our everyday lives because it connects people worldwide and changes how we communicate, work and participate in political and social rights. The growing spread of technology becomes especially evident in developing countries like India. There, the Internet functions as an important center for mobile commerce and provides a powerful platform that empowers citizens to freely express their views and actively engage with their own government. However, the digital landscape constantly is evolving presenting a growing number of threats to individual privacy and democratic principles.

India presents a paradox case in digital governance and surveillance practices. There is troubling contradiction between India's status as the world's largest democracy, with a constitution that enshrines privacy as a fundamental right, and the government's routine engagement in invasive digital surveillance of its own citizens.[1] Privacy is defined as a fundamental right through judicial interpretation rather than explicit text While privacy is not explicitly mentioned in the Indian Constitution, the Supreme Court has interpreted Article 21's guarantee of 'life and personal liberty' to include the right to privacy.[2] The Pegasus spyware revelations exposed how Indian authorities exploit systemic flaws, legal loopholes, and lack of oversight to illegally spy on journalists, activist, and dissidents, disregarding constitutional guarantees.[3] The contradiction and scale of surveillance became evident when the Pegasus

[1] Soumya Lenka, "Article 21 And Its Ever Expanding Scope," *Legal Service India E-Journal*, n.d., https://www.legalserviceindia.com/legal/article-15808-article-21-and-its-ever-expanding-scope.html.
[2] Lenka, "Article 21 And Its Ever Expanding Scope."
[3] Soutik Biswas, "Pegasus: Why Unchecked Snooping Threatens India's Democracy," *BBC News*, 2021, https://www.bbc.com/news/world-asia-india-57887300.

Project revealed over 300 Indian numbers in a leaked database, which included opposition leaders, media figures, activist, and ministers.[4]

The scale and advances of surveillance raises important questions about democratic governance in the digital age. Article 21 of the Indian constitution guarantees the fundamental right to privacy,[5] which the supreme court upheld as absolute in the Puttaswamy vs Union of India case.[6] However, the Indian government has provided minimal transparency or accountability regarding its surveillance practices, citing national security interests despite the lack of judicial oversight under Indian laws.[7] The primary problems here include the inadequate parliamentary and judicial oversight, the very broad exemptions allowing surveillance without sufficient justification, the lack of transparency and accountability mechanisms, the unchecked powers of the security agencies, and the absence of meaningful amendments for citizens targeted by this unlawful monitoring.

This research seeks to identify the primary factors contributing to this divergence in surveillance practices through a comparative analysis with the European Union's GPDR framework, examining key variables: constitution, laws, policies/regulations, diversity of populations, and security considerations. This study aims to identify the institutional and structural factors that enable surveillance overreach despite democratic safeguards. Understanding these dynamics can help democracies worldwide protect civil liberties in a growingly digitalized world.

---

[4] Amnesty International and Forbidden Stories, "About the Pegasus Project," *Forbidden Stories*, n.d., https://forbiddenstories.org/about-the-pegasus-project/.
[5] Lenka, "Article 21 And Its Ever Expanding Scope."
[6] "India: Spyware Use Violates Supreme Court Privacy Ruling," *Human Rights Watch (HRW)*, August 26, 2021, https://www.hrw.org/news/2021/08/26/india-spyware-use-violates-supreme-court-privacy-ruling.
[7] "India: Dangerous Backsliding on Rights Activists, Critics Targeted; Growing Attacks on Muslims, Groups at Risk," *The Human Rights Watch*, 2022, https://www.hrw.org/news/2022/01/13/india-dangerous-backsliding-rights.

This thesis is organized into five chapters that examine the contradiction between India's democratic status and its surveillance practices. Following the first introduction chapter, chapter 2 explores the digital right landscape and the history of surveillance in India, analyzing the hybrid model of internet governance, constitutional frameworks, legislative evolutions, and the impacts there have been on civil society as a whole because of it all. Chapter 3 then divers inot the outline of the methodology used in this research, Mill's Most Similar System Designs (MSSD) and explains the five variables selected to be examined: constitution, laws, polices/regulations, diversity, and security. Chapter 4 then presents a comparative analysis between India and the European Union using these five variables to help identify factors that enables surveillance overreach despite having democratic safeguards. Lastly in the final chapter 5 there is a summary of the findings, comments on the implementations for democratic governance in the digital age and recommendations for future research on the topic.

Technology Overview

The Internet has become integral to India's daily life, the quickly growing digital technology has completely changed how the population of over 1.4 billion people communicate, conduct business, and participate in civic engagement.[8] This digital transformation has resulted in the Internet's evolution form just a simple communication tool to becoming a hub for an important infrastructure. Digital integration in India and globally encourages new and unmatched connectivity and countless opportunities. However, it has also generated new vulnerabilities and challenges when it comes to protecting citizen's privacy and security.

[8] "India Explore All Countries," 2025, https://www.cia.gov/the-world-factbook/countries/india/#introduction.

India has led the world with 1.2 billion internet users since 2023.[9] The Internet penetration rate has continued to grow from 13% in 2014 to 55% in 2025 which means that more than half of the population in India now currently has access to the Internet.[10] This digital growth has transformed rural areas because 442 million Internet users in 2023 reside in rural areas compared to approximately 378 million users in urban regions.[11] This also highlights the rapid growth of digital adoption happening all throughout India. The amount of people who owned some form of smartphone rose to over 97% of Internet users and as of January 2024, India's percentage of web traffic from mobile phones was 79%.[12] The significance of India's Internet usage and technology landscape is in the global digital influence India has due to its populations growing penetration on the Internet while also creating the world largest potential surveillance ecosystem. This rural dominated user based extends surveillance and monitoring capabilities into areas that were previously disconnected. This also means that citizens are carrying surveillance vulnerable devices which only continues to create digital dependency that can also allow for more potential monitoring to occur.

The case of India shows the contrast between digital empowerment and surveillance vulnerability. The very same digital infrastructures that allows the Indian population to participate in e-governance initiatives and also digital commerce also provides mechanisms for state surveillance. It is important to understand the technological landscape before trying to examine the surveillance tools and techniques used in India. Understanding the technology

[9] "Internet Usage in India," *Statista*, 2024, https://www.statista.com/study/22628/internet-usage-in-india-statista-dossier/.
[10] Tanushree Basuroy, "Internet Penetration Rate in India from 2014 to 2025," *Statista*, 2025, https://www.statista.com/statistics/792074/india-internet-penetration-rate/.
[11] "Internet Usage in India."
[12] "Internet Usage in India."

provides context for how these surveillance technologies are being able to be used to exploit digital dependencies.

Pegasus Spyware Technical Capabilities

Pegasus is among the most advanced surveillance tools available on the market, using advanced infiltration technologies and comprehensive data extraction capabilities. This spyware uses multiple infection pathways. It is famous most of all for its zero-click exploits which require no interaction whatsoever from a target. The 2019 WhatsApp incident revealed that several vulnerabilities existed in the operating system being exploited. This resulted in a large number of devices being compromised. Phones were exploited even when targets didn't answer a phone call or open a text message.[13] These capabilities demonstrate the technical capabilities of the tool to bypass traditional security measures that were believed to protect users.[14] Pegasus' most significant technical achievement is its ability to overcome encryption. The data is intercepted by Pegasus directly from the device and interception occurs either before the encryption process or after the decryption process has been completed, instead of an attempt being made to forcibly break the encryption protocols. This exploit method affects popular encrypted messaging apps like WhatsApp, rendering ineffective end-to-end encryption protections because data is collected, unencrypted, at rest.

After Pegasus has been installed the attacker has almost complete control of the compromised device due to the tool's extensive capabilities and comprehensive data access

[13] Stephanie Kirchgaessner, "Court Orders Maker of Pegasus Spyware to Hand over Code to WhatsApp," *The Guardian*, 2024, https://www.theguardian.com/technology/2024/feb/29/pegasus-surveillance-code-whatsapp-meta-lawsuit-nso-group.
[14] Kim Zetter, "Pegasus Spyware: How It Works and What It Collects," *Zero Day*, 2021, https://www.zetter-zeroday.com/pegasus-spyware-how-it-works-and/.

abilities.[15] The attackers are able to retrieve all the stored data, including contacts, messages, and emails from the targeted device. It also allows for real time monitoring of communications while still allowing for the remote activation and control of the device's camera and microphone for surveillance purposes. The GPS location tracking also offers continuous monitoring of the target's movements and access to passwords and other credentials allows for the operator to have access and infiltrate other connected accounts of the target. Pegasus can also monitor both cellular and WiFi network activities. Access to the targets phone provides a detailed glimpse of the target's entire digital life. The spyware operates with extreme stealth because of its advanced compression techniques and advanced transmission methods that limit its data footprints to "a few hundred bytes."[16] This makes Pegasus' activities almost impossible to detect by observing any typical usage patterns or data consumption monitoring.

Pegasus's technical advance demonstrates constant improvement and evolution with more and more new ways to infect systems. The BLASTPASS exploit chain in late 2023 revealed some of the most advanced deployment methods that are capable of compromising even fully updated iOS devices.[17] This kind of attack method uses malicious image attachments, sent using iMessage and uses PassKit framework to compromise a device without any user interaction at all. Making any traditional security practices basically completely useless.[18] The challenge of detecting Pegasus infections varies by platform.[19] Amnesty International created several

[15] Zetter, "Pegasus Spyware: How It Works and What It Collects."
[16] Zetter, "Pegasus Spyware: How It Works and What It Collects."
[17] "BLASTPASS NSO Group IPhone Zero-Click, Zero-Day Exploit Captured in the Wild," *Citizenlab*, 2023, https://citizenlab.ca/2023/09/blastpass-nso-group-iphone-zero-click-zero-day-exploit-captured-in-the-wild/.
[18] "BLASTPASS NSO Group IPhone Zero-Click, Zero-Day Exploit Captured in the Wild."
[19] "Forensic Methodology Report: How to Catch NSO Group's Pegasus," *Amnesty International*, 2021, https://www.amnesty.org/en/documents/doc10/4487/2021/en/.

detection tools, but their effectiveness differs across platforms.[20] iOS devices keep considerably more detailed logs which helps assist in identifying attempted compromises. The differences in detection capabilities among the different platforms highlights an urgent security challenge. While iOS devices provide forensic traces that help identify compromise attempts, the lack of consistent diagnostic capabilities across all mobile platforms underscores the need for device manufactures to develop better auditing and detection tools that would allow device manufactures to develop better diagnostic tools that would allow device owners and other experts to be able to perform better checks.

Prevention methods have changed in response to all these new threats. Apple introduced a lockdown mode which is a considerable improvement in the effort to protect against advanced spyware. This new feature restricts potentially vulnerable channels that Pegasus and other similar tools like to exploit, this includes message attachments and just-in-time (JIT) JavaScript compilations.[21] Newly enhanced security measure reduce a few functions and offer increased protection to high-risk persons, including journalists, activists, and other civil society members. Pegasus attacks typically require three key components: initial exploit chain to gain access, a payload delivery system, and a command and control infrastructure that will support the continuous surveillance. The BLASTPASS discovery showed how these different components work together using the seemingly harmless PassKit attachments as the delivery method while exploiting zero-day vulnerabilities to gain and maintain the continuous access to the target's device.[22]

---

[20] "India: Damning New Forensic Investigation Reveals Repeated Use of Pegasus Spyware to Target High-Profile Journalists," *Amnesty International*, 2023, https://www.amnesty.org/en/latest/news/2023/12/india-damning-new-forensic-investigation-reveals-repeated-use-of-pegasus-spyware-to-target-high-profile-journalists/.

[21] "BLASTPASS NSO Group IPhone Zero-Click, Zero-Day Exploit Captured in the Wild."

[22] "BLASTPASS NSO Group IPhone Zero-Click, Zero-Day Exploit Captured in the Wild."

Recent investigations revealed how significant the extent of Pegasus surveillance is in India. Forensic analysis uncovered new targets including Siddharth Varadarajan, the founding editor of the Wire, as well as Anand Mangnale, South East Asia Editor at the Organized Crime and Corruption Report Project.[23] These cases continue to demonstrate a growing pattern of surveillance targeting journalists.[24] Pegasus surveillance effects not only individual privacy but also has an even greater and broader threat to press freedom and civil society. When a journalist has their device compromised the surveillance endangers more than just their privacy, it also threatens the safety of their sources and weakens their capacity to perform investigative reporting. This produces a chilling effect on journalism. It is also important to note that India uses Pegasus but that it is not the only country that utilizes this surveillance tool.[25]

India's use of Pegasus began in 2017, when the first attacks were recorded.[26] The overall scope of surveillance has expanded since then. More than twenty journalists and other opposition leaders each received Apple's state sponsored attack notifications during October 2023.[27] Repeated attacks on at least several previously identified victims, for example Varadarajan, who experienced an attack in 2018 followed by a second attack in 2023, indicating that there is continued surveillance efforts still focused on specific high-profile targets.[28]

[23] "India: Damning New Forensic Investigation Reveals Repeated Use of Pegasus Spyware to Target High-Profile Journalists."
[24] "India: Damning New Forensic Investigation Reveals Repeated Use of Pegasus Spyware to Target High-Profile Journalists."
[25] International and Stories, "About the Pegasus Project."
[26] "India: Damning New Forensic Investigation Reveals Repeated Use of Pegasus Spyware to Target High-Profile Journalists."
[27] "India: Damning New Forensic Investigation Reveals Repeated Use of Pegasus Spyware to Target High-Profile Journalists."
[28] "India: Damning New Forensic Investigation Reveals Repeated Use of Pegasus Spyware to Target High-Profile Journalists."

The absence of transparency and accountability surrounding these kinds of operations is concerning. Despite investigations by India's Supreme Court, and many repeated revelations of surveillance abuses, authorities still have not offered clarity regarding the use of Pegasus spyware. The lack of clarity provided by the government to its people combined with the nature of these attacks has created distrust and uncertainty, that could challenge the practice of journalism within India's democratic society.

Pegasus surveillance is continuing to evolve. In 2019, WhatsApp discovered that Pegasus had been used to target 1,400 users.[29] This lead to WhatsApp filing a lawsuit against the NSO Group, and in 2024 a US court ordered NSO Group to provide spyware codes as part of that lawsuit.[30] The WhatsApp incident revealed the vulnerabilities that allowed attackers to inject spyware onto its targets devices by simply just sending a phone call to the target's device. [31] This discovery brought about a public attention to the scope of the issue and also brought together NSO Group tools to help. The historical timeline of Pegasus reveals the dramatically increasing pattern of misuse. Over one hundred instances of abusive targeting in at least twenty countries were identified by Citizen's Lab's investigations within Africa, Asia, Europe, Middle East and North America.[32] These attacks were continued even after NSO was obtained by Novalpina Capital which had publicly committed to preventing this kind of misuse.[33] However, these

[29] Soumyarendra Barik, "Pegasus: 300 of 1,400 Users from India, Why Ruling May Re-Open Tapping Debate," *The Indian Express*, 2024, https://indianexpress.com/article/business/whatsapp-pegasus-ruling-us-india-9737575/.
[30] Kirchgaessner, "Court Orders Maker of Pegasus Spyware to Hand over Code to WhatsApp."
[31] "NSO Group / Q Cyber Technologies," *Citizen Lab*, 2019, https://citizenlab.ca/2019/10/nso-q-cyber-technologies-100-new-abuse-cases/; "Indian Journalists Targeted by Israeli Spyware Again: What Do We Know?," *Aljazeera*, 2023, https://www.aljazeera.com/news/2023/12/28/indian-journalists-targeted-by-israeli-spyware-again-what-do-we-know.
[32] "NSO Group / Q Cyber Technologies."
[33] "NSO Group / Q Cyber Technologies."

attacks continue even after ownership changes and public promises of reform which only further demonstrates how powerful the systematic nature of this kind of surveillance.

Surveillance methods have progressed from basic social engineering techniques to advanced zero-click attacks. Early forms of the attacks relied on deceiving individuals by convincing them to click on to malicious links. Operators for example sent messages that would appear to come from trusted contacts or appeared to contain some kind of urgent information about family members.[34] The technology would progress from this to include at capabilities like the WhatsApp vulnerability. This vulnerability did not require any user interaction at all to be able to successfully compromise a device. One pattern that is persistent is the consistent targeting of members of civil society, specifically journalists, human right defenders and other political dissidents. Although NSO Group claims that its technology serves solely legitimate law enforcement purposes, evidence reveals at least several instances of it use against civil society targets instead.[35] This continued targeting despite the large public outcry seems to indicate a disconnect between the company's stated intentions and the actual application of the surveillance technology and tools in practice.

Impact and Scale

The way Pegasus has changed from a specialized intelligence tool to the widespread surveillance system it is today represents the significant development in digital surveillance abilities. Investigations in the Pegasus Project revealed over 100 cases of abusive targeting across several countries including India.[36] And these cases continue to grow. In India alone the

[34] "NSO Group / Q Cyber Technologies."
[35] "NSO Group / Q Cyber Technologies."
[36] International and Stories, "About the Pegasus Project."

surveillance has targeted key members of society demonstrating the pattern of targeting high profile individuals.[37] These targets are not randomly selected, they are comprised of journalists, politicians, civil society leaders, and other high profile peoples that could potentially produce a large amount of intelligence for the operators.

The cross-platform usage of Pegasus makes it capable of compromising both iOS and Android devices, leaving very few mobile users safe. This large and flexible technical capacity combined with the continued development of exploitation methods creates a surveillance equipment that is consistently exceeding any defensive measures in place. Even though security patches solve one vulnerability a new one will emerge which makes sustaining a persistent surveillance capacity a difficult thing to create permanently. The impact of this reaches many entities beyond just individual targets. When a journalist's phone becomes compromised and infected all of their sources are leaked. If an activist's device is compromised, then all of their network is vulnerable to or if an opposition politician is being surveilled then democratic processes are weakened. This effect considerably transforms Pegasus from just a tool into a much more powerful instrument that is capable of changing the relationship between citizen and state power in the digital age.

[37] International and Stories, "About the Pegasus Project."

Chapter 2: Digital Rights and the History of Surveillance in India

In an era of rapid datafication and digital development, India's approach to handling digital rights and surveillance presents a serious paradox. As the world's largest democracy with constitutional protections for privacy, India has still expanded state surveillance powers that challenge the very protections they promise to protect.[38] This chapter examines digital rights and surveillance practices in India through three categories: legal frameworks, policy implementation, and cultural impact. India has experienced dramatic growth in Internet connectivity and digital services, and it is advancing e-governance initiatives. India has over 800 million Internet users.[39] India represents one of the world's largest and fastest-growing digital populations, and this rapid digitalization is accompanied by expanding state control over the digital sphere through the use of surveillance practices that create significant concerns about how civil liberties and democratic values are being protected. The 2021 Pegasus spyware revelations revealed how Indian authorities were allegedly using surveillance tools against their citizens, journalists, activists, and opposition figures, which was a direct contradiction of the Indian constitutional right to privacy and freedom of expression.[40] The tension that exists between democratic principles and surveillance practices in India shows itself in multiple areas and affects many different aspects of life. In the legal sphere, Article 21 of the Constitution enshrines privacy as a fundamental right,[41] and the landmark Puttaswamy judgment of 2017 reinforces this right,[42] yet recent legislation like the Digital Personal Data Protection Act grants broad exemptions for government surveillance;[43] furthermore, India

[38] "PART III FUNDAMENTAL RIGHTS," *The Constitution of India*, 1967, https://www.mea.gov.in/Images/pdf1/Part3.pdf.
[39] Annapurna Roy, "How India Is Using the Internet," *The Economic Times*, 2024, https://economictimes.indiatimes.com/tech/technology/how-india-is-using-the-internet/articleshow/108354854.cms?from=mdr.
[40] Biswas, "Pegasus: Why Unchecked Snooping Threatens India's Democracy."
[41] "PART III FUNDAMENTAL RIGHTS."
[42] "Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors.," *Privacy Library*, 2017, https://nluwebsite.s3.ap-south-1.amazonaws.com/uploads/justice-ks-puttaswamy-ors-vs-union-of-india-ors-5.pdf.
[43] Anirudh Burman, "Understanding India's New Data Protection Law," *Carnegie India*, 2023, https://carnegieindia.org/2023/10/03/understanding-india-s-new-data-protection-law-pub-90624.

has created frameworks for cybersecurity and data protection, but these frameworks often lack strong oversight mechanisms and safeguards against government overreach. Documented surveillance cases target civil society actors and create a climate of self-censorship while destroying the public's trust in their democratic institutions, which shows the cultural impact of these contradictions.

In this chapter the three sections focus on the analysis of digital rights and the history of surveillance in India by first examining how India's legal framework governing digital rights and surveillance has evolved from its original constitutional foundations and has changed with recent legislation. Next, it examines how laws are implemented by looking at surveillance infrastructure and, oversight mechanisms, and enforcement patterns. Lastly, the ethnic and social effects of surveillance practices on civil society and democratic participation are examined at to try to evaluate human rights. This analysis concentrates on how India's approach is differs from similar democratic systems. This chapters the aim is to demonstrate that while India's surveillance practices focus at maintaining social cohesion and national security, they strengthen state power and undermine individual rights. This analysis aims contextualize how India's digital governance model affects human rights and democratic freedoms in the digital age.

India's Hybrid Model of Internet Governance

India's approach to Internet governance represents a special combination of digital control and regulation that conventional categorizations of state control. Models of Internet governance are often used to organize nations into categories ranking levels of state control, India is a complicated reality. The Four Internets framework is applied to analyze multiple elements of global Internet governance approaches and how they have all been selectively adopted and changed by India while its own unique characteristics are developed in its place.[44] India's digital governance framework shows four main patterns of hybridity and,

[44] Kieron O'Hara and Wendy Hall, "Four Internets : Data, Geopolitics, and the Governance of Cyberspace," *Oxford University Press*, 2021, https://doi.org/10.1093/oso/9780197523681.001.0001.

in doing so, also draws attention to the importance of each pattern. This hybridity is shown in how India has strategically combined elements that would have typically been considered contradictory to traditional government models. India's adopts the Silicon Valley model of digital innovation and technical improvement while at the same time implementing several strict regulations that then differ from the models open Internet approach.[45] Similarly, India's data protection regulations follow the language and structure of the Brussel's model.[46] But India's implementation allows for wide ranging state exemptions which is more like the Beijing model.[47] India also seems to utilize some of the Washington DC's commercial model, by embracing digital market developments but again at the same time India still maintains state intervention which is not a feature present in the commercial model.[48]

In India despite protecting privacy in the constitution and other democratic institutions, surveillance capabilities and control mechanisms similar to authoritarian approaches to Internet governance are currently being implemented and misused. The contradiction between democratic principles and authoritarian control are visible in the use of invasive spyware, specifically the NSO developed Pegasus spyware against journalists and activists by the Indian government and by the broad exemptions for state surveillance written in the DPDP Act 2023.[49] This tension is further demonstrated by India's regulatory approaches to protective private sector data while simultaneously expanding state access to citizen date. This illustrates the ongoing contradictory story of democratic principles and authoritarian controls clashing together in India. The duality of the contradiction between democratic principles and authoritarian controls is shown in how strict compliance requirements are imposed on

[45] O'Hara and Hall, "Four Internets : Data, Geopolitics, and the Governance of Cyberspace."
[46] O'Hara and Hall, "Four Internets : Data, Geopolitics, and the Governance of Cyberspace."
[47] O'Hara and Hall, "Four Internets : Data, Geopolitics, and the Governance of Cyberspace"; "India: Spyware Use Violates Supreme Court Privacy Ruling"; "India: Data Protection Bill Fosters State Surveillance," *Human Rights Watch*, 2022, https://www.hrw.org/news/2022/12/23/india-data-protection-bill-fosters-state-surveillance.
[48] O'Hara and Hall, "Four Internets : Data, Geopolitics, and the Governance of Cyberspace."
[49] Raktima Roy and Gabriela Zanfir-Fortuna, "The Digital Personal Data Protection Act of India Explained," *Future of Privacy Forum*, August 15, 2023, https://fpf.org/blog/the-digital-personal-data-protection-act-of-india-explained/.

companies by the DPDP Act and yet broad exemptions for government surveillance activities are continuously granted.[50] Selective regulation of different parts of regulatory and authoritarian governance models are combined together in India. India enables wide-ranging content control and surveillance capabilities that can restrict free expression and privacy while at the same time selectively applying Internet openness and innovation principles and maintaining very strong mechanisms for state intervention that promote digital entrepreneurship and technical advancement.[51]

The patterns of hybridity found in the case of India creates tension and continues to shape India's digital governance frameworks. Fundamental contradictions are created when digital rights are both being protected and violated. Both market-driven innovation and state control coexist and produces a complicated set of governance India's hybrid approach provides critical insights into how emerging powers are trying to navigate competing pressures in digital governance. The subsequent analysis of this chapter focuses on this framework and on understanding how the Indian model functions in legal structures, policy implementation, and cultural impacts.

Laws and Constitutional Framework

Constitutional Foundations

Article 21 of the Indian constitution states, "No person shall be deprived of his life or personal liberty except according to procedure established by law." [52] Although privacy is not specifically mentioned in this article, it has been interpreted to include privacy through multiple court case decisions by the Supreme Court of India. Article 21 is important because it now protects both the physical privacy, informational privacy, decisional autonomy, and digital rights of Indian citizens.[53] The Supreme Court's unanimous decision in Justice K.S. Puttaswamy v. Union of India marked a landmark moment for privacy

[50] Roy and Zanfir-Fortuna, “The Digital Personal Data Protection Act of India Explained.”
[51] “India: Spyware Use Violates Supreme Court Privacy Ruling.”
[52] “PART III FUNDAMENTAL RIGHTS.”
[53] “Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors.”

rights in India and fundamentally reshaped the constitutional landscape of privacy rights in the India.[54] The court ruled that privacy is a fundamental right, stated that privacy protections must change to meet the new digital challenges confronting the nation; the case also found that invasions of privacy must be lawful and serve a legitimate purpose.[55]

The Puttaswamy case's judgment impacts how surveillance practices are conducted because emphasizing the serious need for privacy rights and sets a precedent for stricter regulations. It was established that any government surveillance program must have a legal basis and must also include establish stronger procedural safeguards to prevent abuse so that the rights of Indians continued to be protected.[56] It is also required that programs be designed to be proportionate to the need, and must use the least intrusive means to achieve their goals, while still including mechanisms for oversight as a way to address and correct course when violations do occur.[57] The gap between the constitutional principles and current surveillance practices is evident in the government's continued alleged use of Pegasus spyware.[58] The Puttaswamy judgment requires that surveillance be both lawful and proportionate, the deployment of intrusive spyware against journalists, activists, and other opposition figures is a severe violation of both requirements. Pegasus spyware can access all information on a target's device and can also activate cameras and microphones and monitor real-time communications, this kind of invasive spyware represents the kind of disproportionate privacy invasion that the Court sought to prevent.

The Indian government's response to privacy concerns shows that there is a contrast between constitutional protections and surveillance practices. The Puttaswamy case and judgment declaring privacy as a fundamental right closely mirrors the European Union's approach to digital rights by reflecting elements of the "Brussels' Bourgeois Internet model."[59] The judgment from the Puttaswamy

[54] "India: Spyware Use Violates Supreme Court Privacy Ruling."
[55] "Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors."
[56] "Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors."
[57] "India: Spyware Use Violates Supreme Court Privacy Ruling."
[58] "India: Spyware Use Violates Supreme Court Privacy Ruling."
[59] O'Hara and Hall, "Four Internets : Data, Geopolitics, and the Governance of Cyberspace."

case stresses the importance and also draws attention to the need greater balance between surveillance and the need for strong privacy protections. In ways that echo the GDPR. The implementation of these principles shows how India is actively adopting a hybrid approach to Internet governance and that arise to balance elements of control and freedom. Although India has adopted the language and framework of European-style privacy protection, India's practice of surveillance closely resembles Beijing's authoritarian model. [60] Authorities frequently deploy intrusive surveillance capabilities with minimal safeguards under the guise that they are invoking these surveillance programs to protect national security concerns.[61] The reality is that state authorities are attempting to avoid disclosing details about surveillance programs and trying to avoid implementing strong safeguards to maintain surveillance capabilities.

Despite the emphasis on transparency and accountability established by the Puttaswamy judgment, national security concerns are frequently used by authorities to avoid disclosing details about surveillance programs or to avoid implementing stronger safeguards.[62] The continued deployment of intrusive surveillance suggest that constitutional principles are systematically circumvented. [63] Moreover, indicating minimal regard for the proportionality and procedural safeguards required by the Court when it comes to the exercise of surveillance powers.[64] Although the Supreme Court has created strong protections for privacy as a fundamental right and, particularly within the digital sphere, these protections are not enough to stop the ongoing surveillance abuses of the state. The gap between constitutional principles necessitating the examination of the legislative framework that enables surveillance and how it has evolved in response to technological changes and security challenges.

[60] O'Hara and Hall, "Four Internets : Data, Geopolitics, and the Governance of Cyberspace."
[61] Amrit Dhillon and Michael Safi, "Indian Supreme Court Orders Inquiry into State's Use of Pegasus Spyware," *The Guardian*, 2021, https://www.theguardian.com/news/2021/oct/27/indian-supreme-court-orders-inquiry-into-states-use-of-pegasus-spyware.
[62] "India: Spyware Use Violates Supreme Court Privacy Ruling."
[63] "Forensic Methodology Report: How to Catch NSO Group's Pegasus."
[64] "India: Spyware Use Violates Supreme Court Privacy Ruling."

Legislative Evolution

Pre-2023 Framework

India's digital rights and surveillance legislation reflects the state's ongoing attempts to try to balance security concerns and technological advancements. Pre- 2023 there was four key laws and policies supporting India's cybersecurity and digital rights frameworks. These laws and policies were missing protections against government surveillance. India's first important step toward digital governance was marked by the Information Technology (IT) Act of 2000.[65] The IT Act initiated important changes in how technology is used. The IT Act primarily regulates electronic commerce and addresses cybercrime by creating basic frameworks for things like digital signatures, electronic records, and cybersecurity. However, the provisions regarding privacy and data protection were limited and primarily focused only on unauthorized access and data theft from private actors while neglecting to address anything about government surveillance.[66] Section 69 of the Information Technology Act allowed government agencies powers to intercept, monitor, and decrypt digital communications with executive authorization.[67]

The 2008 Amendment to the IT Act made the law shift by expanding digital regulation and government surveillance powers [68] and creating the Computer Emergency Response Team (CERT-In) as India's national agency for cybersecurity incident response. [69] Although the CERT-In's strengthen India's cybersecurity infrastructure it also had a negative effect by also broadening surveillance capabilities the

[65] "Information Technology Act, 2000," 2000, https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMjk4NzY=#:~:text=%5B9th%20June%2C%202000%5D%20An,communication%20and%20storage%20of%20information%2C.

[66] "Information Technology Act, 2000."

[67] Amnesty International and Citizen Lab, "India: Human Rights Defenders Targeted by a Coordinated Spyware Operation Summary Introduction," *Amnesty International*, 2020, https://www.amnesty.org/en/latest/research/2020/06/india-human-rights-defenders-targeted-by-a-coordinated-spyware-operation/.

[68] Khyati Tejpal et al., "Cybersecurity: Pressing Priority in India," *Journal of Distance Education and E-Learning* 11, no. 2 (n.d.), https://tojdel.net/journals/tojdel/articles/v11i02b/v11i02b-42.pdf.

[69] Tejpal et al., "Cybersecurity: Pressing Priority in India."

program added new provisions allowing for monitoring and collecting traffic data and requiring service providers to help government agencies intercept information.[70] The lack of safeguards set a troubling precedent as the state struggled to protect against abuse due to a concentration on security concerns over privacy rights.

The regulatory framework further developed as by the Information Technology (IT) Rules in 2011 and revised later in 2021 were implemented.[71] The 2011 IT Rules set guidelines for corporations on collecting and storing personal information. and, in doing so, created basic data protection standards. A 2021 revision of the IT Rules further expanded government control over digital spaces. The new rules required social media platforms to help identify messages originators and required these platforms to comply with government takedown requests within strict timeframes.[72] Many critics argued after the 2021 revision of the IT Rules that these requirements for social media platforms were building a surveillance system that could be used to unjustly monitor and control online discourses.[73]

The Department of Electronics and Information Technology published the National Cyber Security Policy in 2013, which represents India's first comprehensive approach to digital security.[74] The policy concentrated on protecting important information infrastructures, and it promoted stronger security awareness.[75] However, as with previous legislation, the policy primarily focused on only external threats and did not give much attention to how citizens needed to be protected from state surveillance. The policy implementation mechanisms were mostly only voluntary and seriously lacked enforcement provisions and accountability measures for government agencies. Each piece of legislation continued to add layers to India's digital governance structure, and expanded state surveillance powers without corresponding increases in accountability or judicial oversight. This framework revealed important gaps in privacy

[70] Tejpal et al., “Cybersecurity: Pressing Priority in India.”
[71] “The Information Technology Rules, 2011,” April 11, 2011.
[72] Tejpal et al., “Cybersecurity: Pressing Priority in India.”
[73] “The Information Technology Rules, 2011.”
[74] Tejpal et al., “Cybersecurity: Pressing Priority in India.”
[75] Tejpal et al., “Cybersecurity: Pressing Priority in India.”

protection and a lack of surveillance oversights needed to protect citizens from state surveillance. India's digital governance structure expanded state surveillance powers as each piece of legislation continued to add layers to India's digital governance structures without increasing accountability or judicial oversight. The framework's emphasis on security over privacy rights created an environment in which surveillance could occur with minimal checks and balances, and this set the stage for the controversies that would emerge alongside the undemocratic use of technologies like Pegasus spyware.

Digital Personal Data Protection Act 2023

After years of gradual digital rights legislation, the Digital Personal Data Protection (DPDP) Act was enacted by India in 2023, The DPDP considered to be the state's most meaningful attempt to create and establish a complete and comprehensive data protection framework.[76] The DPDP was heavily inspired by the European Union's GDPR. The DPDP introduces several new definitions and regulatory mechanisms for personal data protection. Although the DPDP strengthens protections against private sector data breaches, it still allows exemptions for government surveillance activities. The DPDP Act broadly defined personal data as "any data about an individual who is identifiable by or in relation to such data," and because of this broad definition that included both direct identifiers and data that could lead to identification when combined with other information.[77] The DPDP covers automated and partially automated data processing operations. It also included the coverage of activities within India and cross-border data transfers related to Indian goods and services.[78] This scope demonstrates there is an effort to regulate data practices that affect Indian citizens both at home and around the world, and it aims to

[76] Raktima RoyGabriela Zanfir-Fortuna and Gabriela Zanfir-Fortuna, "THE DIGITAL PERSONAL DATA PROTECTION ACT OF INDIA, EXPLAINED," *The Future of Privacy Forum*, 2023, https://fpf.org/blog/the-digital-personal-data-protection-act-of-india-explained/.
[77] Lok Sabha, "Report of the Joint Committee on the Personal Data Protection Bill," 2021, https://prsindia.org/files/bills_acts/bills_parliament/2019/Joint_Committee_on_the_Personal_Data_Protection_Bill_2019.pdf.
[78] Zanfir-Fortuna and Zanfir-Fortuna, "THE DIGITAL PERSONAL DATA PROTECTION ACT OF INDIA, EXPLAINED."

guarantee that these practices are fair and responsible. Explicit consent must be obtained by data fiduciaries before collecting or processing personal data under the DPDP but, the DPDP also allows data processing without consent under multiple circumstances because it includes important exceptions through "legitimate uses" provisions.[79] These exceptions create potential loopholes that could be used to exploit state surveillance objectives.

India's hybrid approach to Internet governance is shown through the nation's legislative framework. Although the DPDP's data protection provisions at first glance resemble the EU's regulatory model, India's continuous ability to grant broad government exemptions and provide limited safeguards seems to more closely align with the Beijing's authoritarian approach to Internet control.[80] The DPDP shows this duality in how government surveillance is treated and how strong protections against private sector data collection exist and are given alongside these wide-ranging and comprehensive state surveillance powers. The structure and creation process of the Data Protection Board (DPB) further reveals how India seems to lean towards this hybrid model because it resembles European regulatory bodies in form, but it lacks independence from government control, making it function more like an authoritarian governance framework.

The DPB serves as the primary oversight mechanism where the government directly appoints the DPB's members which differs from other independent regulatory bodies.[81] The Board has several responsibilities, including monitoring compliance with the DPDP provisions and, investigating data breaches and privacy violations and, imposing penalties for those who do not non-compliance, and also hears grievances from the people.[82] The structure of the DPB has raised concerns regarding the Board's

[79] Burman, “Understanding India’s New Data Protection Law.”
[80] O’Hara and Hall, “Four Internets : Data, Geopolitics, and the Governance of Cyberspace.”
[81] Roy and Zanfir-Fortuna, “The Digital Personal Data Protection Act of India Explained.”
[82] Roy and Zanfir-Fortuna, “The Digital Personal Data Protection Act of India Explained.”

autonomy and ability to regulate government surveillance activities effectively because it weakens the board's autonomy.[83]

The broad exemptions for government entities laid out in the DPDP have been the source of controversy and has raised important questions regarding the fairness and accountability of the DPDP.[84] The DPDP allows government agencies to sidestep privacy obligations because of the prioritization of alleged national security purposes. It also allows for the prevention and investigation of crimes and also to be able to maintain public order and manages foreign relations.[85] These exemptions actively enhance and could actually broaden the government's ability and capability to conduct surveillance as they follow the continuing trend illustrated in previous laws and legislation that places more priority on security concerns rather than on privacy rights. The enforcement framework mainly targets private sector violations, and it has limited mechanisms for challenging government surveillance, and it lacks independent judicial oversight for surveillance activities, also lacks transparency when it comes to reporting requirements for government data collection. The provisions in the DPDP collectively suggest that while the DPDP advances India's data protection framework it also still maintains and potentially reinforces state's surveillance capabilities instead of creating strong safeguards to protect against government overreach. The limitations of the DPDP highlight a broader pattern going on in Indian digital governance, where security concerns consistently tend to supersede privacy protections despite the existence of India's constitutional guarantees of privacy rights.[86]

[83] Anirudh Burman, "The Withdrawal of the Proposed Data Protection Law Is a Pragmatic Move," *Carnegie India*, 2022, https://carnegieindia.org/2022/08/22/withdrawal-of-proposed-data-protection-law-is-pragmatic-move-pub-87710.
[84] "India: Data Protection Bill Fosters State Surveillance."
[85] Burman, "Understanding India's New Data Protection Law."
[86] Sabha, "Report of the Joint Committee on the Personal Data Protection Bill"; Burman, "Understanding India's New Data Protection Law."

Surveillance Legal Framework

India's legal framework for surveillance is a complicated web of legislative provisions, executive orders, and regulatory mechanisms that give wide-ranging powers to government agencies while only providing minimal safeguards against abuse. This framework was developed through multiple pieces of legislation and different administrative orders. It reveals significant gaps in oversight and accountability that desperately need to be addressed. Section 69 of the Information Technology (IT) Act is a key foundation that enables authorities to monitor and control online activities effectively, India's digital surveillance powers rely heavily on this Act.[87] This provision gives government agencies the power to intercept and monitor information and the power to decrypt any data transmitted through any computer resource. These broad definitions and the frequent need for interpretations allow for these terms to be used to justify wide surveillance activities, as the law stipulates that such surveillance must only be necessary for maintaining national security, public order and for investigating crimes.[88]

The Unlawful Activities Prevention Act (UAPA) further extends the state's surveillance capabilities through its anti-terrorism provisions, which have allowed for greater monitoring of activities under the guise that they may threaten national security.[89] The government has used the UAPA to help justify the surveillance of activists, journalists, and other opposition figures in spite of the UAPA's intended focus on preventing terrorist activities. Amnesty International reported that the broad application of the law extends beyond its stated purpose because only 2.2% of UAPA cases resulted in convictions between 2016 and 2019.[90] Surveillance can occur with minimal accountability because the UAPA's provisions allow for extended detention periods and limited judicial oversight. The Ministry of Home Affairs has issued several orders to expand surveillance powers and increase oversight. In 2018, the government

[87] International and Lab, "India: Human Rights Defenders Targeted by a Coordinated Spyware Operation Summary Introduction"; "Information Technology Act, 2000."
[88] "India: Data Protection Bill Fosters State Surveillance"; "Information Technology Act, 2000."
[89] "INDIA: ARRESTS, RAIDS TARGET CRITICS OF GOVERNMENT," *Amnesty International*, 2023, https://www.amnesty.org/en/documents/asa20/7303/2023/en/.
[90] "INDIA: ARRESTS, RAIDS TARGET CRITICS OF GOVERNMENT."

authorized ten central agencies to intercept and, monitor, and decrypt information from any computer resource.[91] These agencies were intelligence organizations, tax authorities, and law enforcement bodies. Critics have opposed the UAPA because of its broad scope and lack of oversight mechanisms and yet it still remains in effect while giving these agencies extensive surveillance authority.[92]

The current legal framework in India suffers from many gaps in privacy protection and surveillance oversight. Based on the investigations conducted by Amnesty International, the current legal frameworks in place seriously lack sufficient safeguards to protect against abuse, and they also allow for government surveillance to be conducted without checks and balances in place.[93] Citizens are left vulnerable to privacy violations and data breaches in the absence of robust data protection laws; this absence continues to compromise their safety. The DPDP's exemption for government entities creates a double standard where private companies are subjected to much stricter regulations than the government entities. The government has greater freedom when it comes to accessing personal data, but because of these deficiencies in the legal frameworks, there are severe effects on the rights and freedoms of the Indian citizens. The use of intrusive spyware by the Indian government was revealed through the Pegasus Project revelations. The alleged use of intrusive spyware by the Indian government to target journalists, activists, opposition politicians, and government critics. Showing how unchecked surveillance powers can lead to the suppression of dissent and self-censorship and a chilling effect on free speech and press freedom.[94] There is a chilling effect on free speech and press freedom when governments use invasive spyware on their citizens. The effects harm democracy and erode public trust and, leading to the suppression of dissent and self-censorship.[95] The gaps and deficiencies in the legal framework allow the use of Pegasus

[91] International and Lab, "India: Human Rights Defenders Targeted by a Coordinated Spyware Operation Summary Introduction."
[92] "INDIA: ARRESTS, RAIDS TARGET CRITICS OF GOVERNMENT."
[93] "India: Damning New Forensic Investigation Reveals Repeated Use of Pegasus Spyware to Target High-Profile Journalists."
[94] International and Stories, "About the Pegasus Project"; "INDIA: ARRESTS, RAIDS TARGET CRITICS OF GOVERNMENT."
[95] International and Stories, "About the Pegasus Project"; "INDIA: ARRESTS, RAIDS TARGET CRITICS OF GOVERNMENT."

spyware against civil society actors, and this shows how weak safeguards can lead to serious privacy violations.[96] The framework emphasizes executive discretion over judicial oversight and combines broad exemptions with limited accountability measures, which creates undesirable conditions where political powers can misuse surveillance for political purposes rather than for legitimate security concerns.

Policies and Implementation

Surveillance Infrastructure

India's surveillance framework is created through the combination of elements from multiple Internet governance models but principles reflects characteristics of both Beijing's authoritarian approach and Brussels' regulatory framework.[97] Similarly to China's extensive surveillance infrastructures, India has also been utilizing and developing more and more sophisticated technical capabilities to use for state monitoring. This is shown in the state's utilization and deployment of advanced tools such as Pegasus spyware. Amnesty International's forensic analysis confirmed that devices belonging to journalists like Siddharth Varadarajan and Anand Mangnale were being targeted. These surveillance practices in India seem to align more with authoritarian governance models than with democratic models. [98] The government coordinates the usage of these tools and requires telecommunications and Internet service providers to retain data which is similar to the Beijing model. [99]

India's surveillance framework shows a sophisticated technical infrastructure that links limited oversight mechanisms and creates a system that allows wide-ranging state monitoring with minimal accountability for those abusing it. India has evolved its surveillance capabilities from basic wiretapping, to more advanced forms of surveillance and digital monitoring tools. Pegasus spyware technology

[96] International and Stories, “About the Pegasus Project.”
[97] O’Hara and Hall, “Four Internets : Data, Geopolitics, and the Governance of Cyberspace.”
[98] HANAN ZAFFAR and JYOTI THAKUR, “How India’s Government Uses Pegasus to Spy on Journalists,” *Freedom Press*, 2024, https://ijnet.org/en/story/how-indias-government-uses-pegasus-spy-journalists.
[99] O’Hara and Hall, “Four Internets : Data, Geopolitics, and the Governance of Cyberspace.”

represents an advanced and powerful capability for surveillance and tracking.[100] Amnesty International confirmed through their forensic analysis that spyware was being utilized to actively target journalists.[101] Pegasus allows its users to access targets devices and conduct real-time surveillance of communications, location data, camera and microphone. Amnesty International and the Citizen Lab uncovered a coordinated spyware campaign that targeted nine human rights defenders in India between the time frame of January to October 2019.[102] Human rights defenders received spear phishing emails with malicious links to install the invasive NetWire spyware onto their computers. NetWire is an invasive spyware is available on Windows. Investigators from Amnesty International and the Citizen Lab documented that tools like NetWire have been used against human rights defenders, like Bhima Koregaon.[103] Mandatory data retention requirements for telecommunications and Internet service providers create a repository of citizen data accessible to government agencies. Access to this data raises concerns about privacy and surveillance, especially because data collection operates through many different channels. According to the IT Rules, social media platforms are required to help identify message originators and comply with government information requests.[104]

India's oversight structure for surveillance activities shows that it diverges from democratic models of Internet governance even though India has implemented several institutional forms that are similar to European regulatory bodies. Although India's implementation adopts institutional forms similar to European regulatory bodies, it more closely resembles Beijing's state-controlled Internet model, which values social stability and government oversight while allowing economic innovation.[105] India's continuous application of surveillance powers within the executive branch without any meaningful

[100] "India: Damning New Forensic Investigation Reveals Repeated Use of Pegasus Spyware to Target High-Profile Journalists."
[101] ZAFFAR and THAKUR, "How India's Government Uses Pegasus to Spy on Journalists."
[102] International and Lab, "India: Human Rights Defenders Targeted by a Coordinated Spyware Operation Summary Introduction."
[103] International and Lab, "India: Human Rights Defenders Targeted by a Coordinated Spyware Operation Summary Introduction."
[104] "The Information Technology Rules, 2011."
[105] O'Hara and Hall, "Four Internets : Data, Geopolitics, and the Governance of Cyberspace."

judicial authorization or independent oversight further demonstrates how India has been adopting authoritarian control mechanisms while maintaining the appearance of having democratic governance structures. The hybrid approach is put on full display when looking into the Right to Information Act's exemptions for national security concerns, frequently providing the necessary blockage to prevent efforts to get information about surveillance policies and further showing a mix of democratic transparency and authoritarian restrictions.[106]

India currently has weak oversight structures for surveillance activities. India fails to guarantee proper monitoring and accountability. Surveillance powers are held by the executive branch as outlined in the 1885 Telegraph Act and the 2000 Information Technology (IT) Act. The branch has unchecked and broad authority to conduct surveillance without judicial authorization or independent oversight. The Supreme Court ruled in 1997 and in 2017 that surveillance orders used only when "strictly necessary" and when there are no alternatives. The lack of independent scrutiny and reporting mechanisms has resulted in accountability issues.[107] The newly established Data Protection Board (DPB) under the DPDP Act exercises limited authority over government surveillance activities.[108] Although private sector data breaches can be investigated by the Board, its jurisdiction over state surveillance is limited by broad national security exemptions that restrict its authority. The Board's appointment processes also raises questions about its independence and overall integrity.

The Supreme Court's technical committee has faced significant obstacles arising from a lack of government corporation with its Pegasus investigation. Even when the courts do intervene, their orders tend to lack any real effective ways to be enforced.[109] Transparency in surveillance operations is severely limited, which negatively affects accountability efforts. Agencies are not required to disclose who their surveillance targets are, even after the operations are completed. Attempts to obtain information about

[106] "India: Spyware Use Violates Supreme Court Privacy Ruling."
[107] "India: Spyware Use Violates Supreme Court Privacy Ruling."
[108] Burman, "Understanding India's New Data Protection Law."
[109] "India: Damning New Forensic Investigation Reveals Repeated Use of Pegasus Spyware to Target High-Profile Journalists."

surveillance practices are again frequently blocked by the national security exemptions within the Right to Information Act, which in return continues to obstruct transparency.[110] This vagueness extends to parliamentary oversight, with limited reporting requirements for surveillance activities.

Policy Implementation Patterns

Data collection practices are extended beyond individual targeting as they are implemented through multiple methods. Human Rights Watch has documented how the Indian authorities have increasingly used surveillance tools and draconian counterterrorism laws and tax raids and foreign funding regulations to monitor and control civil society organizations.[111] These practices often collect wide-ranging personal and organizational data and lack clear legal justification and oversight. Government agencies continue to keep information sharing protocols remain unclear because they do not communicate clearly. The DPDP Act sets guidelines for data processing but the broad exemptions allow for government entities to allow agencies to share information collected through surveillance with minimal transparency and accountability.[112] The erosion of privacy through unregulated spyware usage is violated by democratic principles, freedom of speech and press and association are all stifled, even though they are all constitutionally protected in India.[113]

The enforcement patterns of surveillance-related laws reveal concerning trends and show the need for reform. The pattern of surveillance primarily targets civil society actors, with prolonged detentions and systematic monitoring suggesting these laws serve more as tools for control than legitimate security purposes. As documented by Human Rights Watch, authorities have systematically targeted minority communities, activists, and government critics. [114] Multiple mechanisms are used for this targeting, such

[110] "India: Spyware Use Violates Supreme Court Privacy Ruling."
[111] International and Lab, "India: Human Rights Defenders Targeted by a Coordinated Spyware Operation Summary Introduction."
[112] "India: Data Protection Bill Fosters State Surveillance."
[113] "PART III FUNDAMENTAL RIGHTS."
[114] "India: Dangerous Backsliding on Rights."

as direct surveillance through tools like Pegasus and indirect monitoring through social media platforms and telecommunications data. The government has shown limited cooperation and transparency in its response to legal challenges regarding surveillance because it continuously seeks to control the narrative. When a technical committee was appointed by the Supreme Court to investigate Pegasus usage, the investigation went to a halt because the government "did not cooperate" with the investigation, and the public remained undisclosed to the committee's findings.[115] These implementation patterns show how India's surveillance framework, in spite of constitutional privacy protections, enables the systematic monitoring of civil society with minimal accountability or oversight.

Cultural and Social Impact

The cultural and social impact of platform power represents one of the most profound transformations in how society organizes, communicates, and engages in civil society. Social media platforms are becoming more and more dominant in public discourse and social interactions because their influence extends far beyond just the technological changes and is fundamentally reshaping civil society and democratic participation. Think about how dramatically social media has changed the way we live, connect, and participate in society through the usages of platforms like Instagram, Facebook, Twitter/ X, TikTok, and WhatsApp. These social media platforms haven't just given us new ways to share photos or chat with friends but has also in doing so completely transformed how we debate, share information or news, and engage in protests, these platforms have completely and drastically altered activism and communication. There are several different examples for how states are attempting to handle these powerful platforms around the world. For example, in America the primary focus tends to be on people being able to make money. The Silicon Valley model wants to push to keep things open and free.[116] Another example is in Europe where the focus is on protecting individual rights and Europe accomplishes

[115] "India: Damning New Forensic Investigation Reveals Repeated Use of Pegasus Spyware to Target High-Profile Journalists."
[116] O'Hara and Hall, "Four Internets : Data, Geopolitics, and the Governance of Cyberspace."

this by enforcing strict rules and safeguards. China is another example of a different approach that is more controlling and zeros in on the states own interests, state-centered approach. Each of these three different models are examples of how states around the world and each shapes culture and society in different ways.

Impact on Civil Society

Technology has dramatically changed the way people participate in civil society from Platform power and digital governance from how people communicate, organize, and participate in democracy. These new digital tools have created new opportunities and new challenges for civil society organizations, democratic institutions and citizen participation. Recent documented cases demonstrate just how easily digital governance can be weaponized to suppress civil society participation. In the case of India authorities have systematically targeted many activities, journalists and civil society leaders with technical tools. There are some troubling patterns of how digital tools can be used to silence voices of dissent. For example, forensic investigations showed that many critics of the government had incriminating evidence placed on their devices using advanced malware.[117] These targeting efforts were focused on academics, labor lawyers, poets and some religious leaders all who were advocating for marginalized communities. This targeting is not random and is highly calculated which shows again how digital surveillance can be used to silence diverse civic voices.

Another tool of censorship rather than just blocking specific sites is to just shut down the Internet entirely. India's digital control extends far beyond just plain surveillance to include more direct forms of restricting civic engagement through the use of Internet shutdowns. There are more Internet shutdowns

[117] Niha Masih and Joanna Slater, "Further Evidence in Case against Indian Activists Accused of Terrorism Was Planted, New Report Says," *The Washington Post*, 2021, https://www.washingtonpost.com/world/2021/04/20/india-bhima-koregaon-activists-report/.

happening in India than in any other country in the region[118] with 23 days of national Internet shutdowns over the last year and thousands of days of blockage across different regions throughout the country.[119] These blackouts almost always correspond to political or social upheaval, with authorities using this control as a tool to gain control of volatile situations. One way that the BJP steps in to deal with these control issues is to shut down regional access to the Internet and then after gaining a foothold on the region and the Internet is slowly reopened back up. This is a super blunt method of exerting state control by controlling access to information and severely impacting civil society demonstrating how India's governance model can shift from subtle surveillance to overt restrictions when deemed necessary for maintain social order.

Digital governance both enables and restricts democratic participation, creating a paradox of sorts as digital platforms create new chances for civic engagement and organizations but these platforms have also handed those in power new powerful tools that can be utilized to monitor and control. Civil society organizations have to navigate an environment filled with digital platforms that can provide them with tools to gain more reach but can also expose them to face greater vulnerabilities. The response of all this from civil society has been very mixed as organizations push back against digital restrictions while still trying to adapt to change. The continuing challenges for meaningful civic participation arise from the lack of transparency and accountability in digital governance in India. Weak data protection laws and the lack of oversight make civil society groups and citizens easy targets for surveillance and control. Raising the question of how can India balance the potential of digital tools while still protecting people's rights to participate in civil society?

[118] Jayshree Bajoria, "India's Digital Governance 'Model' Fails on Rights," *Human Rights Watch*, 2023, https://www.hrw.org/news/2023/09/06/indias-digital-governance-model-fails-rights.
[119] "Global Internet ShutdownBajoria, "India's Digital Governance 'Model' Fails on Rights." s India." *Internet Society Pulse*, pulse.internetsociety.org/shutdowns.

Response and Resistance

The response of civil society to digital surveillance and control reveals the ongoing tension between the different types of Internet governance with India's government demonstrating a hybrid combination of elements from both the EU Brussels bourgeois model as well as the Beijing paternal model in its approach to digital platform and Internet governance. Civil society organizations frequently employ multiple resistance strategies that align with many different aspects of the Internet models: Brussels bourgeois, Beijing paternal, DC commercial and the Silicon Valley open model.[120] Digital rights activists in India have actively targeted the troubling mix of the Beijing authoritarian surveillance as well as the Brussels regulatory frameworks.[121] This hybrid approach enables the state to maintain large control while as the same time giving the impression that they are implementing protective regulations in digital spaces.[122]

In cases like the usage of Pegasus to surveille India's combination of state control wielded through multiple seemingly legitimate regulatory frameworks becomes very clear.[123] While the language and structure is European style protections are adopted the approaches resembles China's state centered control much more closely. The current reforms demonstrate this tension through how regulatory frameworks that seem protective but still allow for invasive state control, laws advocating for data protection by mimicking EU regulations like the GDPR but still maintaining strong surveillance powers for the government, and by including many oversight mechanisms that are actively legitimized instead of being uses to limit state intervention. All of these reforms have continuously failed because they continue to uphold a concerning fusion of authoritarian control and regulatory legitimacy. For example, in the new

[120] O'Hara and Hall, "Four Internets : Data, Geopolitics, and the Governance of Cyberspace."
[121] Bajoria, "India's Digital Governance 'Model' Fails on Rights."
[122] Bajoria, "India's Digital Governance 'Model' Fails on Rights."
[123] "India Targeted High-Profile Journalists with Pegasus Spyware: Amnesty," *Aljazeera*, 2023, https://www.aljazeera.com/news/2023/12/28/india-targeted-high-profile-journalists-with-pegasus-spyware-amnesty?traffic_source=KeepReading.

personal data protection law this hybrid approach is highlighted through the use of EU style language while still preserving and even expanding in some instances state surveillance capabilities.[124]

Analysis and Implications

A complicated story is unfolding throughout this analysis of India's digital governance and surveillance practices, showing how a nation is trying to balance democratic principles with expanding state control. The analysis of legal frameworks, policy implementations, and ethics shows how India has created a hybrid approach that glues together models of Internet governance. This new hybrid model that emerges shows itself in how India actively maintains many democratic institutions as well as multiple regulatory frameworks while also deploying large authoritarian-style surveillance capabilities. India shows tension between protection rights and the want to maintain and expand state power.[125] India has sophisticated digital infrastructures and regulatory mechanisms that are very similar to European frameworks like the GDPR but when it comes to implementation patterns India instead resemble authoritarian approaches of surveillance and control.[126] This hybrid model hold many important implications and moving forward it is important for India to actively face these challenges to help resolve the contradictions within its hybrid model. If not, the current trajectory India is heading in indicates that digital governance tools might only continue to erode rather than improve democratic participation along with civil liberties if there are not reforms made. The implications of this far surpass just effecting India but also effect other emerging democracies as they also try to navigate the balance between digital development, democratic rights and human rights in the digital age.

[124] Bajoria, "India's Digital Governance 'Model' Fails on Rights."
[125] "India: Spyware Use Violates Supreme Court Privacy Ruling."
[126] "India Targeted High-Profile Journalists with Pegasus Spyware: Amnesty."

Table 1: Timeline of key legislation and court decisions

Year	Legislation/Court Decision	Significance
1967	Constitution of India, Article 21	Foundation for privacy rights; states "No person shall be deprived of his life or personal liberty except according to procedure established by law"[127]
2000	Information Technology (IT) Act	India's first digital governance legislation; established basic framework for electronic commerce and cybersecurity

[127] "PART III FUNDAMENTAL RIGHTS."

2008	IT Act Amendment	Expanded government surveillance powers; created Computer Emergency Response Team (CERT-In)
2011	Information Technology Rules	Set guidelines for corporations on collecting and storing personal information
2013	National Cyber Security Policy	India's first comprehensive approach to digital security; focused on protecting information infrastructure
2017	Justice K.S. Puttaswamy v. Union of India	Landmark Supreme Court judgment declaring privacy as a fundamental right; required surveillance to be lawful and proportionate
2018	Government authorization of surveillance	Ten central agencies authorized to intercept, monitor, and decrypt information from any computer resource
2021	IT Rules revision	Required social media platforms to identify message originators and comply with government takedown requests within strict timeframes
2021	Pegasus spyware revelations	Discovery that Indian authorities allegedly used surveillance tools against citizens, journalists, and opposition figures
2023	Digital Personal Data Protection (DPDP) Act	India's most comprehensive data protection framework to date; included broad exemptions for government surveillance

Table 2: Data showing Internet shutdowns in India (2023-2024)[128]

Country	National Shutdown (Days)	Regional Shutdown (Days)	Service Blocking (Days)	Total Shutdown Duration (Days)
India	23	2,609.5	13	2,645.5

Table 3: Comparison chart showing India's governance model vs. other models[129]

	India's Hybrid Model	Beijing's Paternal Model	Brussels' Bourgeois Model	Silicon Valley's Open Model	Washington DC's Commercial Model
Core Values	Balance between state	State sovereignty	Individual privacy and regulation	Openness and innovation	Free markets and minimal regulation

[128] "Global Internet Shutdowns: India," *Internet Society Pulse*, 2024, https://pulse.internetsociety.org/shutdowns.

[129] O'Hara and Hall, "Four Internets : Data, Geopolitics, and the Governance of Cyberspace."

	control and innovation	and social stability			
Data Protection	Strong regulations with broad government exemptions	Limited protections, extensive state access	Comprehensive user rights (GDPR)	Self-regulation with minimal oversight	Industry-led standards with limited regulation
Surveillance	Sophisticated surveillance with democratic rhetoric	Direct state monitoring with minimal constraints	Regulated surveillance with judicial oversight	Limited state access with corporate data collection	Public-private surveillance partnerships
Regulation	Selective censorship and Internet shutdowns	Comprehensive filtering and censorship	Content moderation targeting harmful material	Platform-determined moderation policies	Limited content regulation
Innovation	Promotes entrepreneurship while maintaining state control	State-directed innovation in approved sectors	Innovation within regulatory boundaries	Maximized innovation with few constraints	Market-driven innovation with corporate leadership
Legislation	IT Act, DPDP Act 2023	Cybersecurity Law, Data Security Law	GDPR, Digital Services Act	GDPR, Digital Services Act	DMCA, sectoral privacy laws
Important Features	Adopts EU-style protections in language while maintaining China-style control in practice	Direct government control of digital sphere	Strong regulatory framework with independent oversight	Maximum freedom with minimal government intervention	Corporate-friendly approach prioritizing economic benefits

Chapter 3: Methodology

Analyzing the evolution of digital surveillance policies and privacy protections frameworks presents significant methodological challenges. It is difficult to assess the development of policies and practices over time within a country. It is even more difficult to assess

the impact of those policies and their implementations. In the absence of this clear quantitative data this paper relies on the comparative method to examine how two democratic systems with similar challenges have developed drastically different approaches to digital surveillance and privacy protections. This comparative approach allows for the identification of the key factors that are contributing to the divergence of outcomes despite the similarities that both systems start with and the similar challenges each state confronts. This study uses a structured comparative framework called Mill's Most Similar Systems Design (MSSD) to analyze how India and the European Union, despite sharing democratic foundations and both facing similar security concerns, have both chosen to implement different surveillance practices and privacy safeguards. By examining these systems that both share multiple characteristic but produce different results in the dependent variable (level of protection against surveillance overreach) this methodology will be able to help identify specific institutional and policy variations that influence the protection of digital rights across jurisdictions, or if it is not a policy issue and the divergence stems from the lack of effective safeguards in practice despite the state's policy commitments.

Mill's Method: Analytical Framework

This study uses Mill's Most Similar Systems Design (MSSD) to conduct a systematic comparative analysis between India and the EU about their digital surveillance practices and privacy protections. MSSD is useful because when researchers seek investigate systems with similarities despite different outcomes in the dependent variable.[130] MSSD provides a framework that allows for the examination of two things that are similar but that also have differing results in

[130] Carsten Anckar, "On the Applicability of the Most Similar Systems Design and the Most Different Systems Design in Comparative Research," *International Journal of Social Research Methodology* 11, no. 5 (2008): 389–401, https://doi.org/10.1080/13645570701401552.

the dependent variables. The level of protection against surveillance overreach and safeguarding of digital rights constitutes the dependent variable in this study. The MSSD method is useful for this research because it helps control for irrelevant variables by focusing on systems sharing multiple characterizes and by deliberately selecting casers with structural similarities allowing for researchers to isolate and examine these specific factors that could point to an explanation to explain the different outcomes. MSSD is most useful and works best when the units of comparison have a lot of in common to use as a baseline, but in the end, they still produce differing results in the study.[131] India is a country, and the EU is a supernational organization. They both function and act as large democratic systems where constitutional principles and legal frameworks apply across diverse populations. By examining cases with many similar features and with different outcomes, MSSD enables for the identification of key causal factors that contribute to the divergence in the surveillance practices as well as privacy protections.

Case Selection: European Union and India

For the purpose of this research, India and the EU are treated as states, although it is important to recognize that the EU is not a state and is in fact a supranational political and economic union that governs lots of actors. India and the EU represent compelling comparative cases for many reasons because firstly they both function as large democratic systems with constitutional commitments to fundamental rights.[132] Second, both the EU and India possess legal frameworks that explicitly recognize privacy rights. Third, both states govern highly diverse populations (multiple languages religions and cultural identities). Fourth, both states face similar

[131] Anckar, "On the Applicability of the Most Similar Systems Design and the Most Different Systems Design in Comparative Research."
[132] "PART III FUNDAMENTAL RIGHTS."

security challenges including terrorism and transnational threats. Fifth, India and the EU both have undergone rapid digital transformation with large online populations. Lastly, the states have significant global economic and political influence in their regions. However, despite these similarities the outcomes regarding surveillance practices and privacy protections differ substantially. The EU has established robust safeguards against surveillance overreach through frameworks like the GDPR, while India has developed a pattern of invasive surveillance despite constitutional guarantees of privacy, this divergence in outcomes makes these cases ideal for MSSD analysis.

The Oxford Handbook of Comparative Politics examines the methodology of comparative politics and offers valuable insights into how we should approach case selection when attempting to identify causal relationships between institutional arrangements and social outcomes.[133] The main challenge for comparative analysis is that, "to identify causal effects, we must rely on some assumptions that are untestable,"[134] this challenge becomes relevant when examining how democratic systems that are similar starts to diverge in privacy protection outcomes. The comparisons of India and the EU uses the most similar systems design and examine cases that share similar backgrounds but still vary in the outcomes. When cases are matched on directly observable covariates, differences within the outcomes may be more plausibly attributed to certain key institutional or policy variations instead of to underlying background conditions. "A necessary condition for identification is path independence: situations where historical paths diverged at some time from the same background conditions of the same kind," India and the EU represent

[133] Adam Przeworski, *' Is the Science of Comparative Politics Possible?', In Carles Boix, and Susan C. Stokes (Eds), The Oxford Handbook of Comparative Politics*, Oxford Handbooks, 2009, https://doi.org/10.1093/oxfordhb/9780199566020.003.0006.
[134] Przeworski, *6 Is the Science of Comparative Politics Possible?*

this kind of scenario described.[135] Both, of them began with constitutional commitments to uphold fundamental rights and privacy, but their paths diverge into to significantly different forms of implementation and institutional developments. This divergence offers a specific opportunity however, "where history was kind enough to have generated different causes under the same conditions,"[136] in addition to allowing the examination of how different institutional arrangements lead to different privacy outcomes despite similar starting points as well as similar challenges.

By looking closely at both of these cases "different values of causes under the same background conditions,"[137] we are able to better comprehend in a lot of detail the exact kind of institutional elements that will strengthen or weaken privacy safeguards in the society of democratic nations. The selection of India and the EU addresses what Przeworski calls the problem of endogeneity.[138] Which is described as, "the difficulty presented by endogeneity is to distinguish the effects of causes from the effects of conditions under which they operate,"[139] here through a selection of cases that exhibit comparable background conditions but that also have different institutional conditions, we are able to begin to isolate the effect of privacy protection mechanisms out of broader sociopolitical contexts that these mechanisms operate within. During the comparison, we cannot assign the privacy protection mechanisms to the political systems, "when we cannot control the assignment of the potential causes, we are at the mercy of history,"[140] but we can analyze how these different institutional choices within the two similar democratic systems have both produced different outcomes.

[135] Przeworski, *6 Is the Science of Comparative Politics Possible?*
[136] Przeworski, *6 Is the Science of Comparative Politics Possible?*
[137] Przeworski, *6 Is the Science of Comparative Politics Possible?*
[138] Przeworski, *6 Is the Science of Comparative Politics Possible?*
[139] Przeworski, *6 Is the Science of Comparative Politics Possible?*
[140] Przeworski, *6 Is the Science of Comparative Politics Possible?*, chap. 6.

Core Variables and Significance

This comparative analysis between India and EU uses five key variables for the explanation of the divergence in surveillance practices despite their similar democratic frameworks. Following MSSD methodology, cases that share multiple similar background conditions but differ in outcomes are examined to identify causal factors. Using case studies, "When analyzing causal relationships this analysis is concerned not only with the strength of an X/Y relationship but also with the distribution of evidence across available cases," it also emphasizes that when analyzing causal relationships in case studies it is important to consider the strength of the X/Y relationship and whether or not the evidence is consistently seen across multiple cases to ensure validity.[141] These variables aim to offer variation in order to explain the divergence in outcomes among otherwise similar cases.

Variable one: Constitution

The constitutional foundations for privacy rights, along with limitations over surveillance, act as a core variable inside this study. Analyzing several specific constitutional provisions shows how fundamental legal principles can empower surveillance activities. These same principles can also limit surveillance activities throughout these systems. This variable is valuable particularly in how it establishes a baseline on legal authority with respect to privacy protections along with the scope of state surveillance. Although India and the EU both acknowledge privacy as a fundamental right in their constitutional frameworks, the understanding and usage of these particular rights differs. The EU's Charter of Fundamental Rights ensures the entitlement for personal data

[141] John Gerring, *"The Case Study: What It Is and What It Does", in Carles Boix, and Susan C. Stokes (Eds), The Oxford Handbook of Comparative Politics*, Oxford Handbooks, 2009, https://doi.org/10.1093/oxfordhb/9780199566020.003.0004.

protections besides privacy (Article 7 and 8),[142] establishing a constitutional foundation that shapes the EU's legislative approach to regulations. By contrast, the privacy protections in India's constitution result from judicial decisions and not from explicit language.[143] The constitution variable assists in identifying how differences among constitutional foundations lead to divergent paths regarding privacy protection despite the similar democratic values.

Variable two: Laws

Laws about surveillance and data protections are an important variable in putting into operation constitutional principles and moving those principles towards enforceable standards. This analysis considers the instruments that are used to regulate surveillance activities, information collection, and privacy protections. The GDPR applies across the EU, establishing the baseline requirements for data protection with clearly defined limitations on data processing,[144] while India's legislative approach includes significant exemptions for state surveillance based on what the government views as importance.[145] Examining this variable, within this context, reveals how somewhat similar democratic systems can produce greatly different legislative outcomes based on how precisely they balance multiple security interests and individual rights. Legislative frameworks also show the institutional path dependencies. These frameworks reflect how regulatory systems effect privacy outcomes. The strength here is specificity as well as enforcement

[142] "EU Charter of Fundamental Rights - Article 8," *Official Journal of the European Union C 303/17*, 2007, https://fra.europa.eu/en/eu-charter/article/8-protection-personal-data; "EU Charter of Fundamental Rights-Article 7," *Official Journal of the European Union C 303/17*, 2007, https://fra.europa.eu/en/eu-charter/article/7-respect-private-and-family-life.
[143] Lenka, "Article 21 And Its Ever Expanding Scope."
[144] Ben Wolford, "What Is GDPR, the EU's New Data Protection Law?," GDPR.EU, 2020, https://gdpr.eu/what-is-gdpr/.
[145] "India: Data Protection Bill Fosters State Surveillance."

mechanisms in these laws directly affect the level with protection citizens experience against surveillance overreach.

Variable three: Policies and Regulations

The institutional structures responsible for implementing and overseeing privacy laws constitute a key variable that translates legal standards into practical protections. This variable examines the independence, authority, and overall effectiveness of regulatory bodies that minor compliance with privacy laws and provide remedies for any violations of them. The EU has developed independent data protection authorities that have large powers to be able to enact and enforce regulations,[146] but the way that India oversees surveillance differs from democratic models because its oversight mechanisms lack independence from government influence.[147] This variable is important to include because even notably strong constitutional and legal protections can be weakened if there is weak implementation in conjunction with weak oversight bodies. Looking into how each system structures its regulatory architecture can give insight into the effectiveness of privacy protections beyond the formal legal guarantees.

Variable four: Diversity

This variable reveals just how surveillance disproportionately targets marginalized communities and how legal frameworks either address or neglect these inequalities. Surveillance technologies interact with existing social inequalities and influence their impact on privacy rights. This becomes complicated because of the interplay between surveillance technologies and

[146] Bradford Anu, "Globalizing European Digital Rights through Regulatory Power," in *Digital Empires: The Global Battle to Regulate Technology*, by Bradford Anu (Oxford Academic, 2023), 324-, https://doi-org.ezproxy.lib.vt.edu/10.1093/oso/9780197649268.003.0010.
[147] "India: Spyware Use Violates Supreme Court Privacy Ruling."

marginalized communities demonstrates continued patterns of state control mechanisms that tend to frequently target specific groups of people. Both in India and the EU there are diverse populations with people who speak multiple languages, practice different religions, and have different cultural identities.[148] Which makes this variable relevant to understanding the impact of surveillance. Helping to reveal if surveillance practices are disproportionately targeting marginalized communities and how legal frameworks are or are not accounting for these inequalities is a crucial aspect of digital rights. The ways in which surveillance technologies interact with social inequalities can also influence the impact on privacy rights too. This variable provides better insights into whether privacy protections are universally applied or if there are groups that are more effected than others, this can also reflect other structural patterns to help answer how surveillance power is disturbed and applied.

Variable five: Security

Security considerations and threat perceptions represent a key element influencing how surveillance is both justified and deployed. This variable examines how each system conceptualizes security concerns and balances essential security practices against privacy protections. India and the EU both face similar security challenges including terrorism and transnational threats. However, both countries have developed different approaches to incorporating privacy safeguards within security operations. The EU usually requires substantially more strict necessity and proportionality assessments,[149] while India's approach frequently grants

[148] Sanat Pai Raikar and Muzaffar Alam, "People of India," *Britannica* 1 (2025): 1–6, https://doi.org/10.1109/ic2em59347.2023.10419441; "Discrimination in the European Union," *Eurostat*, n.d., https://europa.eu/eurobarometer/surveys/detail/2972; "Demography of Europe – 2024 Edition," *Eurostat*, 2024, https://ec.europa.eu/eurostat/web/interactive-publications/demography-2024.
[149] Anu, "Globalizing European Digital Rights through Regulatory Power."

increased leeway for security agencies.[150] This factor helps explain how similar safety issues can lead to different outcomes based on social institutions, historical context, and community perceptions of security risks. The relationship between security and privacy shows the core values and priorities within each of these two democracies.

Roadmap: Integration of Methods and Variables

This comparative analysis between India and the European Union demonstrates how two democratic systems with similar foundational principles can develop significantly divergent approaches to digital surveillance and privacy protection. Through the application of Mill's Most Similar Systems Design (MSSD), this study identifies key variables that contribute to these different outcomes despite the similar challenges both countries face. Constitutional frameworks in India and the EU establish privacy as a fundamental right but regardless of these rights the implementation and interpretation over these rights have followed two different routes. The EU has cultivated large bodies to safeguard principles through frameworks like the GDPR.[151] However, India's approach has been characterized by its gaps between constitutional guarantees with practical implementation. This difference points that constitutional guarantees alone may not be enough to ensure privacy protections. Especially if there is not institutional commitments to protect their enforcement.

This research aims to show how through the use of MSSD, it can be used to reach the goal to find out how certain institutional, legal and cultural things that have an effect on surveillance and privacy inside democracies. We can thoroughly comprehend which things digital rights

[150] "India: Data Protection Bill Fosters State Surveillance"; Burman, "Understanding India's New Data Protection Law."
[151] Wolford, "What Is GDPR, the EU's New Data Protection Law?"

safeguards are most affected by if we inspect situations that are similar but have different outcomes. The data indicates that good privacy safeguards involve more things than constitutional acknowledgement.

Additional research could be done to help broaden the scope of this comparative analysis to include democratic systems or investigate how these privacy protection frameworks systematically change over time when they are confronted with any new technologies. As digital surveillance capabilities ceaselessly continue toward improvement, comprehension of the many institutional factors that either constrain or enable surveillance overreach becomes even more important for the protection of fundamental rights within democratic societies.

This chapter has discussed the method for analyzing two complex socio-political systems and provided an overview of the variables for analysis. Having established the methodological framework, along with the key variables for this study the next chapter will build on this one and provide a detailed comparative analysis of each of the variables and help to distinguish why these seemingly similar institutional frameworks result in divergent outcomes. This comparative analysis will explore the nuances of constitutional interpretations, legislative frameworks, regulatory mechanisms, impact on diversity, and security considerations in both of the two democratic systems. By systematically analyzing these variables, the following chapter will highlight the specific factors that cause these seemingly similar institutional frameworks toward such divergent outcomes in privacy protection as well as in surveillance practice. This examination will aim to help reveal the important institutional and policy variations. These variations determine the effectiveness of privacy safeguards in democratic states that face similar challenges.

Chapter 4: Comparative Analysis

The previous chapter established Mill's Most Similar Systems Design (MSSD) as the methodological framework for comparing the European Union and India regarding digital surveillance

and privacy protection.[152] Despite their shared democratic foundations and similar challenges throughout the digital sphere these two states have both developed very different approaches in balancing security interests and individual privacy rights. This chapter will conduct a comparison across the five variables: constitution, laws, policies and regulations, diversity and security. Through examining each of these variables we are able to identify the various factors that have led these similar democratic systems to diverge in their protection of digital rights.

The EU, with its GDPR and the Digital Service Act, has made itself a leader in privacy protection by imposing strict limitations on data collection and highlighting individual rights.[153] India, despite its constitutional recognition of privacy as a fundamental right, has still developed surveillance frameworks that allow for significant governmental exemptions and limited independent oversights.[154] Through this comparative analysis, the goal is to understand not only how these systems differ but also specifically why they have followed specific paths despite similar starting points. The findings have many important implications for democratic governance in the digital age. The findings offer insights and better understanding into the institutional arrangements that most effectively safeguard privacy and digital rights while still combating legitimate security concerns.

Variable one: Constitutional Comparison

The constitutional foundations of privacy rights within the EU and India offer some interesting differences regarding how democratic systems acknowledge and safeguard basic

[152] Anckar, "On the Applicability of the Most Similar Systems Design and the Most Different Systems Design in Comparative Research."
[153] "At a Glance: Does the EU Digital Services Act Protect Freedom of Expression?," *Article 19*, 2021, https://www.article19.org/resources/does-the-digital-services-act-protect-freedom-of-expression/; Eliška Pírková, "How the Digital Services Act Could Hack Big Tech's Human Rights Problem," *Access Now*, 2020, https://www.accessnow.org/eu-digital-services-act/; "EU: Landmark Digital Services Act Must Be Robustly Enforced to Protect Human Rights," *Amnesty International*, 2024, https://www.amnesty.org/en/latest/news/2024/02/eu-landmark-digital-services-act-must-be-robustly-enforced-to-protect-human-rights/.
[154] "India: Spyware Use Violates Supreme Court Privacy Ruling."

digital rights. While both India and the EU do acknowledge privacy as being a fundamental right, they both differ significantly in the way in which these rights are codified and interpreted. The EU's approach comes from the explicit provisions in the Charter of Fundamental Rights that separately protects both traditional privacy[155] and data protection [156], creating a framework that is very thorough and rooted in constitutional texts. India's privacy rights emerged from judicial interpretations not solely on direct constitutional provisions. The Supreme Court established privacy as part of the "right to life and personal liberty," under Article 21,[157] a distinction like this helps shape of systems balance individual rights against state interests in surveillance and also data collection.

European Union's Constitutional Framework

The EU believes that privacy and data protection are at the highest level of the legal hierarchy, and this is shown through the explicit codification in the Charter of Fundamental Rights. It is important to note that when this paper refers to the 'EU constitutional framework,' I am addressing the collection of treaties that function as the EU's constitution rather than a single constitutional document. Article 7 of the Charter guarantees that "everyone has the right to respect for his or her private and family life, home and communications," this establishes privacy as a fundamental right for all.[158] Article 8 goes even further by specifically dealing with personal data protection stating that "everyone has the right to the protection of personal data concerning him or her."[159] This explicitly separates the two and creates a dual protection system that recognizes both customary privacy concepts as well as modern data protection needs. This

[155] "EU Charter of Fundamental Rights- Article 7."
[156] "EU Charter of Fundamental Rights - Article 8."
[157] Lenka, "Article 21 And Its Ever Expanding Scope"; "Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors."
[158] "EU Charter of Fundamental Rights- Article 7."
[159] "EU Charter of Fundamental Rights - Article 8."

constitutional framework establishes clear principles for the EU to govern data collection and processing, including the requirements for consent and for other independent oversights. The Court of Justice of the European Union has additionally and substantially expanded these protections through important landmark decisions. In the 2014 case called Digital Rights Ireland, the court invalidated fully the Data Retention Directive, which highlighted that mass surveillance measures must be reasonably proportionate and must also include proper safeguards.[160] Similarly in another case called the Court of Schrems I and II, the court also prioritized EU citizens' data protection over commercial and international cooperation interests, which voided pacts for data sharing with the United States.[161]

India's Constitutional Framework

India's constitutional protection for privacy follows a very different path. Unlike the EU, India's Constitution contains no explicit mention of privacy. Article 21 simply and clearly states that "no person shall be deprived of his life or personal liberty except according to procedure established by law."[162] For decades, this omission left privacy rights in a state of uncertainty, and there were conflicting judicial opinions about whether privacy was constitutionally protected. The Justice K.S. Puttaswamy v. Union of India judgment definitively resolved this ambiguity when a nine-judge bench in the Supreme Court unanimously recognized privacy as a fundamental right.[163] The Court held that privacy is an intrinsic part of the "right to life and

[160] "The Court of Justice Declares the Data Retention Directive to Be Invalid," *Court of Justice of the European Union*, 2014, https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf; "How Digital Rights Ireland Litigated Against the EU Data Retention Directive and Won," *Electronic Frontier Foundation*, 2014, https://doi.org/10.1016/j.clsr.2006.05.005.
[161] Hendrik Mildebrath, "The CJEU Judgment in the Schrems II Case," *European Parliamentary Research Service*, 2020, https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf; Maria José Rangel de Mesquita, "The Court of Justice of the European Union," *Vox EU*, 2020, 451–67, https://doi.org/10.1163/9789004298712_027.
[162] "PART III FUNDAMENTAL RIGHTS."
[163] "Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors."

personal liberty" under Article 21.[164] Privacy was also proven to apply to other freedoms guaranteed by the Constitution and Justice Chandrachud's shared his view that underscored how privacy is, "the constitutional core of human dignity" and includes personal intimacies, personal choices, and informational privacy.[165] However, this right still lacks the explicit parameters and limitations found in the EU Charter. The Puttaswamy judgment, while revolutionary, also acknowledged that privacy is not an absolute right and established a fairness test for restrictions, leaving significant flexibility in future cases.[166]

Impact of the Constitutional Approaches

The contrast between the explicit codification in the EU and judicial derivation in India has large implications for privacy protection implementation. First, the EU's explicit approach provides clarity as well as certainty for citizens. For policymakers and courts, this approach offers even greater clarity. This clarity has enabled the development of legislation. The GDPR comprehensively and directly implements constitutional principles. In contrast looking at India's implied approach has resulted in a more fragmented and occasionally contradictory implementation, as lawmakers and courts continue to interpret the boundaries of this right. Second, the respective roles of constitutional courts can differ considerably between these various systems. The CJEU has often focused on interpreting and applying already-established constitutional provisions. This pattern then leads to the continual reinforcement of privacy norms over the years. On the other hand, the Supreme Court of India has played a role that is more foundational, and it has created essentially the constitutional basis for privacy rights instead of interpreting existing provisions.

---

[164] "PART III FUNDAMENTAL RIGHTS."
[165] V. Shivshankar, "Privacy an Essential Aspect of Human Dignity, Says Supreme Court in Historic Ruling," *The Wire*, 2017, https://thewire.in/law/supreme-court-right-to-privacy-verdict.
[166] Lenka, "Article 21 And Its Ever Expanding Scope."

Lastly, the EU's decision to treat data protection as a completely separate fundamental right has enabled much more targeted and technologically relevant protections. This distinction has acknowledged the different challenges posed by digital data processing and established a separate constitutional basis for regulating it which avoids misinterpretations and confusion. In India, both traditional privacy and modern data protection concerns fall under exactly the same derived right, potentially limiting the overall development of specialized protections for digital contexts and allowing room for ambiguities in how data protection is interpreted and enforced. This fundamental difference in constitutional architecture, explicit and differentiated in the EU versus implicit and derived in India, establishes the foundation for the divergent approaches to privacy protection that we observe throughout their legal and regulatory systems.

Variable two: Legal Framework Analysis

Building upon both India and the EU's own constitutional foundations, India and the EU both have developed considerably different legal frameworks for data protection and for surveillance regulations. These frameworks reflect each states own specific approaches to balancing individual rights alongside with state interests. The EU's GDPR represents a right centered approach that focuses on prioritizing privacy for citizens across all sectors, while on the other hand India's legislative landscape that is more fragmented features exemption after exemption of importance for activities of government surveillance. These divergent legal structures point to the fundamental differences in how each democracy views the relationship of individual data rights to government authority. These legal frameworks establish certain practical mechanisms and through it constitutional privacy principles are able to be implemented and enforced through regulation.

European Union's Legal Framework

The EU has established a comprehensive and unified legal framework that prioritizes individual rights while also setting clear boundaries for both private and governmental data processing. The General Data Protection Regulation (GDPR) encompasses this framework, which came into effect in 2018 and is still the strongest data protection law globally.[167] The GDPR establishes several core principles governing the personal data processing including: lawfulness, fairness, transparency, purpose for limitation, data for minimization, accuracy, storage for limitation, integrity and confidentiality, and also accountability.[168] These principles apply uniformly across all EU member states; in addition, they extend beyond EU borders to any organization processing EU citizens' data.[169] The regulation grants people powerful rights, including full access to their data, rectification of any inaccuracies, erasure, restriction on processing, data portability, as well as objection to some certain types of processing.[170]

Beyond the GDPR, the EU has developed additional legislation addressing specific aspects of digital rights. The Digital Services Act (DSA) which is signed and implemented, for example, aims to regulate content moderation while protecting fundamental rights, establishing due process requirements and transparency obligations for online platforms.[171] Electronic communication privacy is specifically addressed by the ePrivacy Directive (soon to be replaced by the ePrivacy Regulation).[172] The Law Enforcement Directive provides certain data protection

[167] Wolford, "What Is GDPR, the EU's New Data Protection Law?"
[168] Ismail Özkan, "Data Protection Principles: The 7 Principles Of GDPR Explained," *CyberPilot*, 2001.
[169] Wolford, "What Is GDPR, the EU's New Data Protection Law?"
[170] Wolford, "What Is GDPR, the EU's New Data Protection Law?"
[171] "EU: Landmark Digital Services Act Must Be Robustly Enforced to Protect Human Rights."
[172] "THE EU EPRIVACY REGULATION: WHAT IT IS AND WHAT TO EXPECT," *USERCENTRICS Cookiebot*, 2024, https://www.cookiebot.com/en/eprivacy-regulation/#:~:text=Direct%20marketing%20communications%20under%20the,send%20such%20a%20marketing%20message.

safeguards in the context of criminal investigations along with security operations.[173] A few EU cases laws have continued to strengthen each of these protections. EU case law has also strengthened these protections further. In Google Spain v. AEPD (2014), the CJEU established the "right to be forgotten," mandating search engines to delete links to personal information under specific conditions.[174] The Schrems decisions completely invalidated all data-sharing frameworks with the United States specifically because of certain surveillance concerns, thereby showing the overall primacy of privacy rights even in particular international contexts.[175]

India's Legal Framework

India's legal framework for data protection and surveillance reveals a more fragmented approach with significant exemptions for government activities. Until recently, India lacked thorough data protection legislation and instead relied heavily on various sectoral rules and the Information Technology Act of 2000 (IT Act) and its amendments.[176] The IT Act and the Information Technology Rules gave some protections to "sensitive personal data" handled by corporate entities.[177] However, these rules applied narrowly and lacked strong enforcement mechanisms or thorough coverage of all data processing activities.

---

[173] "THE EU EPRIVACY REGULATION: WHAT IT IS AND WHAT TO EXPECT."
[174] James Ball, "Costeja González and a Memorable Fight for the 'Right to Be Forgotten,'" *The Guardian* 58, no. 1 (2014): 35–37, https://www.theguardian.com/world/blog/2014/may/14/mario-costeja-gonzalez-fight-right-forgotten.
[175] Monika Zalnieriute, "Data Transfers after Schrems II: The EU-US Disagreements over Data Privacy and National Security," *University of New South Wales* 55, no. 1 (2022), https://scholarship.law.vanderbilt.edu/vjtl/vol55/iss1/1/; Mildebrath, "The CJEU Judgment in the Schrems II Case."
[176] Zanfir-Fortuna and Zanfir-Fortuna, "THE DIGITAL PERSONAL DATA PROTECTION ACT OF INDIA, EXPLAINED"; "Information Technology Act, 2000."
[177] "The Information Technology Rules, 2011"; Tejpal et al., "Cybersecurity: Pressing Priority in India."

In 2023, India finally passed the Digital Personal Data Protection Act (DPDPA) after years of back-and-forth deliberation.[178] While the law does mark a step forward for data protection in the country, it comes with a big catch when it comes to government agencies. According to Section 17(2)(a), the government can essentially exempt itself from the law's provisions by notifying certain state instrumentalities that are acting in the interests of things like sovereignty, security of the State, foreign relations,' or public order.[179] These broad exemptions mean that when it comes to government surveillance, citizens might find themselves with far less protection than they'd hoped for under this new law.

India's surveillance legal framework remains primarily governed through the Telegraph Act of 1885 and Section 69 of the IT Act, and these authorize interception of communications and computer resources.[180] These laws permit surveillance based on the broadly defined grounds such as "the interest of the sovereignty and integrity of India" and "friendly relations with foreign states," with authorization coming from executive officers rather than from independent judicial authorities.[181] There are cases that are challenging surveillance including the PUCL v. Union of India (1996), where the Supreme Court established guidelines for telephone tapping in the absence of statutory procedural safeguards.[182] However, all of these judicial interventions have not led to any form of thorough reform for the surveillance frameworks.

[178] "THE DIGITAL PERSONAL DATA PROTECTION ACT," 2023, https://indiankanoon.org/doc/3510545/.
[179] "THE DIGITAL PERSONAL DATA PROTECTION ACT."
[180] "THE INDIAN TELEGRAPH ACT Act No. 13," 1885, https://dot.gov.in/sites/default/files/the_indian_telegraph_act_1985_pdf.pdf; "Information Technology Act, 2000"; "Section 69 in The Information Technology Act," 2000, https://indiankanoon.org/doc/1439440/.
[181] "Section 69 in The Information Technology Act"; "THE INDIAN TELEGRAPH ACT Act No. 13."
[182] Kuldip Singh, "People'S Union Of Civil Liberties ... vs Union Of India (Uoi)," 1996, https://indiankanoon.org/doc/31276692/.

Analysis of Legal Approaches

The contrast between these several legal frameworks reveals certain fundamental differences in approach. The EU adopts a thorough, rights-centered model and applies consistent principles across various industries and multiple actors, including government entities. India employs a more sectoral approach with important exemptions for state activities, particularly those related in security and public order. The contrast between these several legal frameworks reveals certain fundamental differences in approach. The EU system restricts data gathering and handling to only what is most necessary, using these norms even for security actions. India's framework, while acknowledging privacy rights, provides considerably broader discretion to government authorities with very minimal independent oversight. Specific enforcement mechanisms do also differ quite substantially. The GDPR empowers independent Data Protection Authorities with the ability of imposing heavy penalties.[183] The enforcement structure of India under the DPDPA grants large authority unto a Data Protection Board, and its independence from governmental influence is still somewhat questionable.[184]

In most instances, the treatment of security exceptions seems to reveal the differences in priorities between both India and the EU. The EU requires surveillance to meet very strict necessity along with proportionality tests with judicial oversight. In the case of India's legal framework there provides broad exemptions, with limited safeguards. This reflects a clear fundamental difference in how these democratic systems balance individual rights against security interests. These legal framework differences, stemming from constitutional approaches, have led to vastly different levels of protection against surveillance overreach despite the similar democratic foundations.

[183] "Fines / Penalties," *Intersoft Consulting*, n.d., https://gdpr-info.eu/issues/fines-penalties/.
[184] Burman, "Understanding India's New Data Protection Law."

Variable three: Policy and Regulatory Assessment

The effectiveness of privacy and data protection frameworks depends considerably on their implementation by and through regulatory bodies and enforcement mechanisms. The EU along with India exhibit stark differences in their regulatory approaches, reflecting their special constitutional and legal foundations. These regulatory differences are seen in many aspects in the EU's Data Protection Authorities process having significant autonomy while India's Data Protection Board maintains closer ties to government influences.[185] The transparency requirements, accountability structures, and procedural safeguards highlight the priorities. Each one of these two states places contrasting emphasis on individual rights versus state prerogatives. These regulatory frameworks additionally reveal just how abstract legal principles translate into practical oversight of private companies but also government agencies in the collection and retention of personal data.

European Union's Policies and Regulations Framework

The EU has indeed established such a strong, multi-layered regulatory system, one characterized by truly independent oversight and quite strong enforcement powers. At the nationwide level, each member state fully maintains an independent Data Protection Authority (DPA) for enforcing the GDPR.[186] These authorities possess quite broad investigative powers, including the ability for them to conduct multiple audits, access several data processing facilities,

[185] "Legal Framework of EU Data Protection," *European Commission*, n.d., https://commission.europa.eu/law/law-topic/data-protection/legal-framework-eu-data-protection_en#:~:text=EU%20Member%20States%20have%20set,more%20than%20one%20Member%20State.; Burman, "Understanding India's New Data Protection Law."
[186] "Legal Framework of EU Data Protection."

and examine various pieces of equipment. Authorities can issue various warnings, impose temporary or permanent bans regarding processing, and levy meaningful administrative fines reaching up to €20 million or 4% of some organization's global annual revenue.[187]

The European Data Protection Board (EDPB), which has national DPA representatives, makes sure data protection rules are applied consistently across the EU.[188] This cooperative mechanism addresses cross-border cases through a "one-stop-shop" procedure, and it allows for coordinated regulation of multinational entities while maintaining consistent standards across member states.[189] The independence of these regulatory bodies is structurally guaranteed. It is also legally protected. In Commission v. Germany (2010), the CJEU stressed that DPAs "must act objectively and impartially," and therefore "must remain free from any external influence, whether direct or indirect."[190] This independence will also extend to budgetary matters as well as appointment procedures and functional decision-making.

For surveillance activities, the EU regulatory framework usually requires prior authorization from judicial authorities. According to the European Court of Human Rights, surveillance requires "adequate and effective safeguards against abuse," such as oversight from independent groups.[191] Transparency is another cornerstone making up the foundation of EU regulatory policies. In the EU organizations must maintain records of all processing activities

---

[187] "Fines / Penalties."
[188] "The European Data Protection Board," *The European Data Protection Board (EDPB)*, 2022, https://www.edpb.europa.eu/about-edpb/who-we-are/european-data-protection-board_en#:~:text=Search%20on%20the%20EDPB%20web%20site:&text=It%20ensures%20that%20the%20General%20Data%20Protection,as%20the%20European%20Data%20Protection%20Supervisor%20(EDPS).
[189] "The European Data Protection Board."
[190] Golden Data Law, "Commission v. Germany and the Independence of Supervisory Authorities," *Medium*, 2019, https://medium.com/golden-data/commission-v-germany-and-the-independence-of-supervisory-authorities-d64dcb276b9a.
[191] Franziska Boehm, "A Comparison between US and EU Data Protection Legislation for Law Enforcement Purposes," *European Parliament*, 2015, https://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU(2015)536459_EN.pdf.

and conduct thorough Data Protection Impact Assessments (DPIAs) specifically when processing operations are likely to result in a high risk.[192]

India's Policies and Regulations Framework

India's regulatory framework lacks the independence and transparency found in the EU model. While the Digital Personal Data Protection Act (DPDPA) established a Data Protection Board, its structure raises significant concerns about government influence and compromised independence. Unlike EU DPAs with their guaranteed independence, India's Data Protection Board is both appointed by and reports directly to the central government.[193] Government officials control the selection committee and appointment process, raising serious questions about the Board's ability to act independently, particularly when handling cases involving government surveillance.[194]

India's surveillance system operates with almost no independent oversight. Under the Telegraph Act and Information Technology Act, the executive branch wields broad surveillance powers without judicial checks or meaningful safeguards.[195] Despite two Supreme Court rulings limiting surveillance to only, when necessary, the system lacks any real accountability or independent scrutiny.[196] The Central Monitoring System (CMS), Network Traffic Analysis (NETRA), and the National Intelligence Grid (NATGRID) provide the government with meaningful surveillance capabilities, yet these systems still operate with minimal public

[192] "Art. 35 GDPR Data Protection Impact Assessment," *GDPR.Edu*, n.d., https://gdpr.eu/article-35-impact-assessment/.
[193] Burman, "Understanding India's New Data Protection Law."
[194] Burman, "Understanding India's New Data Protection Law."
[195] "India: Spyware Use Violates Supreme Court Privacy Ruling."
[196] "India: Spyware Use Violates Supreme Court Privacy Ruling."

transparency or oversight.[197] The Right to Information Act, which could have provided mechanisms for transparency, still exempts certain intelligence and security organizations.[198]

Court challenges to India's surveillance mechanisms have repeatedly highlighted some serious regulatory issues and shortcomings. Since the Supreme Court recognized privacy as a fundamental right,[199] multiple petitions have challenged surveillance powers under the IT Act and the Telegraph Act.[200] These challenges point to gaps within the system including no oversights, minimal procedure safeguards, and a troubling lack of transparency in how surveillance is being conducted.[201] However, despite the efforts very little has changed at all. The legal framework still remains flawed, and experts are still arguing and saying that India urgently needs, "comprehensive legislation governing the functioning of intelligence and law enforcement agencies."[202] The current practices are still not meeting the requirements that were established by the Supreme Court, and other legislations like Personal Data Protection Bill, with all of these exemptions for law enforcement agencies the problems could just continue to become increasingly worse.[203]

---

[197] Jhalak M. Kakkar et al., "The Surveillance Law Landscape in India and the Impact of Puttaswamy," *National Law University Delhi Press*, 2023, https://ssrn.com/abstract=4624419.
[198] Kakkar et al., "The Surveillance Law Landscape in India and the Impact of Puttaswamy."
[199] Lenka, "Article 21 And Its Ever Expanding Scope."
[200] "'No Internet Means No Work, No Pay, No Food' Internet Shutdowns Deny Access to Basic Rights in 'Digital India,'" *Human Rights Watch*, 2023, https://www.hrw.org/report/2023/06/14/no-internet-means-no-work-no-pay-no-food/internet-shutdowns-deny-access-basic#:~:text=II.,by%20central%20and%20state%20governments.&text=These%20powers%20could%20be%20misused,or%20any%20form%20of%20oversight.
[201] "'No Internet Means No Work, No Pay, No Food' Internet Shutdowns Deny Access to Basic Rights in 'Digital India.'"
[202] Smriti Parsheera and Prateek Jha, "Cross-Border Data Access for Law Enforcement: What Are India's Strategic Options?," *Carnegie India*, 2020, https://carnegieendowment.org/research/2020/11/cross-border-data-access-for-law-enforcement-what-are-indias-strategic-options?lang=en.
[203] Parsheera and Jha, "Cross-Border Data Access for Law Enforcement: What Are India's Strategic Options?"

Analysis of Policies and Regulations

The contrast between EU and Indian regulatory approaches reveals fundamental differences in how privacy rights are protected in practice. Regulatory independence varies quite dramatically between India and the EU. The EU DPAs operate as truly independent entities that empower and challenge government activities, whereas in India the Data Protection Board often lacks this similar structural independence, specifically in cases that might involve government interests. Another example is how surveillance differs, in the EU there is a typical requirement for judicial pre-authorization in almost all cases involving intrusive surveillance. Meanwhile, India instead relies largely on executive authorization.[204] This procedural difference reflects deeper distinctions in how these systems balance privacy rights against security interests for themselves.

Another difference is how enforcement capabilities diverge considerably. EU regulators are able to impose quite meaningful penalties for violations, truly creating meaningful deterrents against privacy infringements. India's enforcement mechanisms still remain quite limited, with questions regarding whether the Data Protection Board shall aggressively pursue violations, especially those involving government entities. Lastly, transparency requirements depict different approaches toward accountability. The EU mandates require transparency from private as well as from public entities regarding data processing activities, while India continues to lack these kinds of transparency requirements, particularly for security-related operations.

These regulatory differences help to explain why these similar constitutional commitments to privacy have still produced such drastically different outcomes between both of these democracies, showing that these outcomes are occurring in practice rather than in

[204] "India: Spyware Use Violates Supreme Court Privacy Ruling."

regulatory measures. The EU's robust and independent regulatory framework transforms legal protections into effective safeguard whereas, India's regulatory system creates for significant gaps between protections and implementation especially when it comes to surveillance oversights.

Variable four: Diversity Considerations

When looking at how the EU and India handle digital privacy it is important not to ignore the human element of this issue specifically how these systems protect or don't protect diverse and vulnerable populations. Privacy isn't experienced the same way by everyone and people from marginalized communities often face greater risks when surveillance systems fail them. Both India and the EU are the home to very incredibly diverse populations with many different languages, cultures, and many different levels of digital literacy and technology access. In India the caste system represents an additional dimension of diversity that needs further exploration in future research. The caste system functions as bureaucratic that significantly impacts rights distribution and access to technological resources.[205] Future studies should examine how this hierarchical social structure influences privacy policy implementation and outcomes within the context of India. But despite these similarities both states have different approaches when it comes to fair protection. This section examines how each system incorporates safeguards against discriminatory surveillance practices and addresses the unique challenges faced by vulnerable communities.

[205] "What Is India's Caste System?," *BBC*, 2019, https://www.bbc.com/news/world-asia-india-35650616.

EU Diversity Framework

The EU has incorporated protections against discriminatory surveillance into its current data protection regime. The GDPR requires organizations to conduct impact assessments for high-risk processing activities, explicitly addressing potential discrimination. Article 22 grants individuals the right not to be subject to solely automated decisions that produce legal or similarly significant effects, this is to try and offer citizens protection against any kind of algorithmic bias that could lead to discrimination.[206] Additionally, the EU's Artificial Intelligence Act proposes several safeguards against discriminatory outcomes from AI systems in addition, classifying certain applications as "high-risk" when deployed in sensitive contexts.[207]

India Diversity Framework

India still lacks safeguards against discriminatory surveillance even though India has such a diverse population including several religious, linguistic, as well as cultural communities now.[208] The exclusion of vulnerable populations is part of a broader pattern of rights concerns in India. Indian authorities intensified their crackdown on activists, journalists, and government critics through politically motivated prosecutions with increasing attacks being directed towards religious minorities, especially Muslims.[209]

Studies have documented significant cybersecurity vulnerabilities in digital identity systems. India experienced what was described as its 'largest data breach' when personal

[206] GDPR, "Art. 22 - Automated Individual Decision-Making, Including Profiling," *Intersoft Consulting*, n.d., https://gdpr-info.eu/art-22-gdpr/.
[207] "EU AI Act: First Regulation on Artificial Intelligence," *European Parliament*, 2023, https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.
[208] Raikar and Alam, "People of India."
[209] "India: Dangerous Backsliding on Rights."

information from the Aadhaar system, including biometric data and personal identifiers on 815 million Indians, was leaked on the Dark Web.[210] This breach exposed citizens to risks of identity theft and financial fraud, highlighting critical concerns about data security and privacy in large-scale digital identification systems.[211] India's Aadhaar data breach exposed biometric and personal information of citizens which only continues to highlight the critical security vulnerabilities in there are in these large-scale digital identity systems.[212]

The Aadhaar digital identity system in India, even while intended to improve access to government services, has created exclusions in welfare administration as well as also presenting dangers to constitutional privacy rights.[213] Digital ID systems can also create significant barriers for marginalized communities. Including people with disabilities, elderly, low income, and those who may struggle with documentation requirements or technology access.[214] These systems often require users to give personal data in exchange for services they should be legally entitled to receive.[215]

Analysis of Diversity

The contrast between these approaches reveals how privacy frameworks differently address structural inequalities. The EU's approach acknowledges that certain privacy violations

[210] Jenna Manhau Fung, ed., "Bridging Divides and Navigating Digital Landscapes: A Study on Internet Access, Cybersecurity, and Sustainable Practices in Asia Pacific," *NetMission Academy Case Study Series*, 2024, 31.
[211] Fung, "Bridging Divides and Navigating Digital Landscapes: A Study on Internet Access, Cybersecurity, and Sustainable Practices in Asia Pacific."
[212] Fung, "Bridging Divides and Navigating Digital Landscapes: A Study on Internet Access, Cybersecurity, and Sustainable Practices in Asia Pacific."
[213] "Use of Entity Resolution in India: Shining a Light on How New Forms of Automation Can Deny People Access to Welfare," *Amnesty International*, 2024, https://www.amnesty.org/en/latest/research/2024/04/entity-resolution-in-indias-welfare-digitalization/.
[214] "Understanding the Risks of Digital IDs," *Immigrant Defense Project*, n.d., https://www.immigrantdefenseproject.org/wp-content/uploads/Digital-IDs-FAQ.pdf.
[215] "Understanding the Risks of Digital IDs."

as well as general surveillance can disproportionately affect vulnerable communities, incorporating safeguards at many different levels to try and stop this from happening. However, the framework in India lacks some of these similar protections, potentially increasing some of the already existing social divides. The difference here is mainly reflecting how across broader institutional approaches toward diversity the EU actively incorporating of non-discrimination principles within digital governance, while India's framework focuses upon universal application without specific protections by communities most vulnerable under surveillance overreach. The different approaches and methods between the two shows just how apparent unbiased privacy structures might lessen or else strengthen current social disparities.

Variable five: Security Implications

When it comes to data privacy, countries have to make tough choices between protecting personal information and keeping citizens safe. This section looks at how the EU and India handle this balancing act in completely different ways. The EU tries to keep security agencies in check with strict judicial oversight and targeted surveillance, while India gives its security forces much more freedom with fewer independent checks. These different approaches make sense when you consider each region's history but what is interesting is how two democratic systems can both value privacy in theory but end up with such different practical approaches to security.

EU Security Framework

The EU has developed security approaches that aim to help balance legitimate security interests while still maintaining strong privacy protections. Central to this framework is the principle that security protocols need to properly meet very strict tests to be able to ensure that

surveillance is being targeted rather than just used broadly. EU law requires that security agencies use the least intrusive means possible to achieve legitimate aims, with measures tailored to specific threats.[216] This is because the EU security framework relies heavily on judicial oversight. Most members of states do require prior judicial authorization for intrusive surveillance measures which creates an independent check on executive powers.

The European Court of Human Rights has stressed the importance of independent review countless times, such as in the case of Weber v. Germany[217] and Roman Zakharov v. Russia.[218] Establishing that surveillance regimes lacking similar oversight violates fundamental privacy rights. Even counter-terrorism measures must also conform to these data protection principles despite pressing security urgency or importance. In the Digital Rights Ireland and Tele2 Sverige cases, the CJEU invalidated mass data retention practices despite their security benefits, showing that security threats alone do not justify disproportionate privacy intrusions.[219]

India Security Framework

India's security framework grants wide ranging leeway to intelligence and law enforcement agencies through very broad exemptions in privacy legislations. The Digital Personal Data Protection Act contains many exemptions for security agencies that are mainly

[216] "The NIS 2 Directive | Updates, Compliance," *NIS 2 Directive*, n.d., https://www.nis-2-directive.com/#:~:text=Stronger%20risk%20and%20incident%20management,of%20large%2Dscale%20cybersecurity%20incidents.
[217] "Weber and Saravia v. Germany: Case Analysis," *Global Freedom of Expression Columbia University*, n.d., https://globalfreedomofexpression.columbia.edu/cases/weber-saravia-v-germany/.
[218] "Krzysztof Brejza v. Poland and 8 Other Applications," *Amnesty International*, 2025, 11, https://www.amnesty.org/fr/wp-content/uploads/2025/02/EUR3790822025ENGLISH.pdf; "CASE OF ROMAN ZAKHAROV v. RUSSIA," *European Court of Human Rights*, 2015, https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-159324%22]}.
[219] "CJEU Declares General Data Retention Unlawful in Tele2 Sverige," *CCDCOE*, 2016, https://ccdcoe.org/incyder-articles/cjeu-declares-general-data-retention-unlawful-in-tele2-sverige/; "How Digital Rights Ireland Litigated Against the EU Data Retention Directive and Won."

made possible due to greatly defined national security grounds. These exemptions put lots of surveillance and monitoring activities outside of the scope of data protections requirements.

Border security and terrorism concerns have driven the expansion of different surveillance technologies, including facial recognition systems which are at borders and even in public spaces. The Central Monitoring System, NATGRID, and further surveillance infrastructure enable wide-ranging data collection with very limited oversight.[220] Counter-terrorism justifications, especially in border regions as well as areas with insurgent activities, have supported large wide-ranging surveillance powers. While the Indian Supreme Court established procedural guidelines for surveillance in cases like PUCL v. Union of India, these safeguards primarily involve internal executive review rather approval through independent judicial authorization.[221] Security agencies here retain a lot of significant discretion when it comes to cases like this, with all the oversight mechanisms being largely limited to just internal governmental controls instead of being fully independent bodies.

Analysis of Security Implications

The EU and India present separate strategies when it comes to weighing security and privacy, which reflects the different conceptions surrounding security threats and priorities. The EU views privacy as improving rather than weakening security, maintaining that targeted surveillance with strong safeguards will ultimately produce better security outcomes rather than having mass surveillance. On the other hand, India's approach prioritizes clear state security interests because privacy protections easily give way to broadly defined security concerns. These

[220] Pameela George, "India's Surveillance Landscape after the DPDPA," *IAPP*, 2025, https://iapp.org/news/a/india-s-surveillance-landscape-after-the-dpdpa.
[221] Sunil Abraham and Elonnai Hickok, "Government Access to Private-Sector Data in India," *International Data Privacy Law* 2, no. 4 (2012): 302–15, https://doi.org/10.1093/idpl/ips028.

divergent paths have arisen from many different historical security challenges. Indias experience with terrorism, boarder conflicts, and uprisings has promoted an approach for security agencies to have greater scopes. The EU's past experiences with totalitarian regimes has also produced increased sensitivity to surveillance overreach even when it is justified by security needs.

The function of courts also varies greatly between the two. In the EU courts actively review and then limit security-based surveillances, which in doing so helps to establish clear boundaries that executive agencies cannot cross regardless of security justifications. In Indian courts, they do recognize privacy as a fundamental right, but they have also shown a greater ability to defer to security-based justifications for surveillance, by focusing on procedural requirements rather than having limitations.[222]

These contrasting approaches show that democratic systems can develop considerably difference balances between security as well as privacy solely on the basis of their institutional traditions, historical experiences, and security priorities. In states like India and the EU even when there are similar constitutional foundations at the beginning that recognize privacy as a fundamental right.

Table 4: Comparing how the EU and India Approach Digital Privacy

Variable	European Union	India
Constitution	Privacy is written directly into EU law through Articles 7 & 8 of the EU	Privacy isn't explicitly mentioned in India's Constitution. The Supreme Court had to step in (Puttaswamy case)

[222] Lenka, "Article 21 And Its Ever Expanding Scope"; "India: Spyware Use Violates Supreme Court Privacy Ruling."

	Charter.[223] Citizens have a clear right to both privacy and protection of their personal data.	to declare it's part of the "right to life" under Article 21.[224] Article 21 of India Constitution: Protection of Life and Personal Liberty[225]
Laws	The EU created comprehensive laws like GDPR that apply everywhere in Europe. These laws strictly limit how organizations can use personal data and give people control over their information. General Data Protection Regulation (GDPR)[226]	India takes a piecemeal approach with different laws (IT Act, Data Protection Act) that have many exceptions for government agencies. The government has much more freedom to collect data. Digital Personal Data Protection (DPDP) Bill[227]
Policies and Regulations	Independent watchdogs (Data Protection Authorities) can investigate and issue huge fines (up to 4% of a company's global revenue). Courts must approve surveillance. Digital Service Act (DSA)[228]	India's enforcement bodies aren't truly independent from government influence. Government officials, not judges, can authorize surveillance with little oversight.

[223] "EU Charter of Fundamental Rights- Article 7"; "EU Charter of Fundamental Rights - Article 8."
[224] "Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors."
[225] "PART III FUNDAMENTAL RIGHTS."
[226] Wolford, "What Is GDPR, the EU's New Data Protection Law?"
[227] Burman, "Understanding India's New Data Protection Law."
[228] "EU: Landmark Digital Services Act Must Be Robustly Enforced to Protect Human Rights."

		Information Technology Act of 2000[229]
Diversity	EU rules require checking whether data systems might discriminate. Companies must explain automated decisions that affect people. EU has a diverse population of over 440 million people from 27 states[230]	Evidence shows minorities and certain communities face more surveillance in India. Digital systems sometimes create extra barriers for already marginalized groups. One of the most diverse countries in the world with a population of over 1.4 billion people[231]
Security	The EU requires that security measures must be necessary and proportionate. EU courts have struck down government surveillance programs for going too far.	India puts national security concerns first, with broad exceptions to privacy protections. There's minimal oversight of surveillance and limited opportunity for courts to review security activities.

Conclusion

Examining at how the EU and India both handle digital privacy along with surveillance it becomes clear that just because two states have similar democratic values does not guarantee than there will be similar outcomes. Even though both states recognize that privacy is vital they both diverge down different paths. These differences aren't only about technical details or legal

[229] "Information Technology Act, 2000."
[230] Eurostat, ed., "Facts and Figures on the European Union," *European Union*, 2023, https://european-union.europa.eu/principles-countries-history/facts-and-figures-european-union_en.
[231] Raikar and Alam, "People of India."

language they also reflect deeper realities about what each state prioritizes based on its history and challenges. A lot can be learned from such a comparison as this. One thing that is proved is that just saying “privacy matters” isn’t enough. Real protection requires strong independent oversight and courts to be willing to stand up to any government overreach. Even when national security is involved. These lessons will continue to be important as countries try to balance security and privacy in this increasingly digital world.

Chapter 5: Conclusion

Summary of Findings

This study reveals contradictions between India’s privacy protection framework and surveillance practices. At the heart of this study is the paradox between India’s status as the world’s largest democracy with constitutional privacy guarantees and its continued deployment of various extensive invasive surveillance tools against citizens, journalists, and political opponents.[232] Although both India and the EU

[232] “PART III FUNDAMENTAL RIGHTS.” “India: Damning New Forensic Investigation Reveals Repeated Use of Pegasus Spyware to Target High-Profile Journalists.”

operate as democratic systems with commitments to privacy their implementations have diverged dramatically. The key difference is not in the stated principles but instead lies within institutional frameworks. Within India surveillance lacks meaningful independent oversight and significant government exemptions are frequent within its data protection frameworks and executive controlled regulatory bodies. The EU on the other hand has fully developed strong safeguards highly independent regulatory authorities and has strict requirements for surveillance operations.[233] In the Pegasus spyware revelations, India's approach exemplifies the enablement of surveillance overreach despite constitutional protections and any accountability.[234] This divergence occurs even despite similar security challenges faced by both states, suggesting that institutional design as well as democratic safeguards, rather than specific security needs, determine surveillance outcomes in most democratic societies.

Implications of Analysis

The findings show that constitutional guarantees are insufficient for the protection of privacy rights in the absence of proper institutional implementation and legal codification. The case of India reveals how surveillance powers can weaken democratic functions when oversight mechanisms remain under executive control. The targeting of journalists and opposition figures via Pegasus spyware has created a chilling effect upon freedom of speech and expression and political participation, weakening democratic accountability.[235] Indias hybrid approach to adopting EU-style regulatory language and to maintaining Beijing-style surveillance capabilities represents a possible model for emulation for other democracies, posing global concerns for digital rights.[236] The contradiction between democratic principles and surveillance practices raises questions about the advancements and changes of state power in digital democracies. As surveillance technologies get better, the gap existing between constitutional

[233] Wolford, "What Is GDPR, the EU's New Data Protection Law?"
[234] "India: Damning New Forensic Investigation Reveals Repeated Use of Pegasus Spyware to Target High-Profile Journalists"; Biswas, "Pegasus: Why Unchecked Snooping Threatens India's Democracy"; "Forensic Methodology Report: How to Catch NSO Group's Pegasus."
[235] "INDIA: ARRESTS, RAIDS TARGET CRITICS OF GOVERNMENT"; "India: Dangerous Backsliding on Rights."
[236] O'Hara and Hall, "Four Internets : Data, Geopolitics, and the Governance of Cyberspace."

protections and actual practices may begin to widen without any real structural reforms focused on independent oversight, judicial authorization, and transparency.

Future Research Recommendations

Future research should explore more specific institutional reforms that can help better align India's surveillance practices with India's constitutional guarantees, particularly focusing on developing oversight bodies that are truly independent and have strong enforcement. Comparative analysis could also extend further beyond the EU to include other democratic systems with similar diverse security challenges to help identify more successful governance models. Research could also expand into examining the effectiveness of judicial interventions to help determine whether courts can push for meaningful surveillance reforms without legislative support. Another avenue would also be technical research to focus on defensive technology to protect against surveillance, maybe focusing on verifications mechanisms, to detect spyware like Pegasus, which would empower civil society to hold governments accountable. Lastly, international regulatory frameworks are needed to help address the nature of cross-border surveillance technologies, this would examine potential international agreements to restrict the sale and use of intrusive spyware against civilians in democratic contexts.

Final Reflections

Overall, this thesis aims to contribute to the understanding of democratic governance by revealing how constitutional protections can be undermined through institutional choices that can then enable surveillance overreach in the digital age. The divergence between India and the EU shows that the health of digital democracy depends not only on stated principles but also on concrete oversight mechanisms, separation of power, and enforcement capabilities. The importance of addressing surveillance overreach cannot be overlooked. Technologies like Pegasus represent a fundamental threat to preserving democratic values, enabling governments to monitor and potentially suppress political opposition, free press, and civil society without any accountability. Regardless of security challenges, all democracies need to develop oversight mechanisms that are strong and independent, posing these enforcement powers

so that constitutional guarantees are protected. The future of democratic governance within the digital age will be determined not by what constitutions promise but by how effective those promises are institutionalized and defended against the ever-expanding capabilities of state surveillance.

Bibliography

Abraham, Sunil, and Elonnai Hickok. "Government Access to Private-Sector Data in India." *International Data Privacy Law* 2, no. 4 (2012): 302–15. https://doi.org/10.1093/idpl/ips028.

Anckar, Carsten. "On the Applicability of the Most Similar Systems Design and the Most Different Systems Design in Comparative Research." *International Journal of Social Research Methodology* 11, no. 5 (2008): 389–401. https://doi.org/10.1080/13645570701401552.

Anu, Bradford. "Globalizing European Digital Rights through Regulatory Power." In *Digital Empires: The Global Battle to Regulate Technology*, by Bradford Anu, 324-. Oxford Academic, 2023. https://doi-org.ezproxy.lib.vt.edu/10.1093/oso/9780197649268.003.0010.

"Art. 35 GDPR Data Protection Impact Assessment." *GDPR.Edu*, n.d. https://gdpr.eu/article-35-impact-assessment/.

"At a Glance: Does the EU Digital Services Act Protect Freedom of Expression?" *Article 19*, 2021. https://www.article19.org/resources/does-the-digital-services-act-protect-freedom-of-expression/.

Bajoria, Jayshree. "India's Digital Governance 'Model' Fails on Rights." *Human Rights Watch*, 2023. https://www.hrw.org/news/2023/09/06/indias-digital-governance-model-fails-rights.

Ball, James. "Costeja González and a Memorable Fight for the 'Right to Be Forgotten.'" *The Guardian* 58, no. 1 (2014): 35–37. https://www.theguardian.com/world/blog/2014/may/14/mario-costeja-gonzalez-fight-right-forgotten.

Barik, Soumyarendra. "Pegasus: 300 of 1,400 Users from India, Why Ruling May Re-Open Tapping Debate." *The Indian Express*, 2024. https://indianexpress.com/article/business/whatsapp-pegasus-ruling-us-india-9737575/.

Basuroy, Tanushree. "Internet Penetration Rate in India from 2014 to 2025." *Statista*, 2025. https://www.statista.com/statistics/792074/india-internet-penetration-rate/.

Biswas, Soutik. "Pegasus: Why Unchecked Snooping Threatens India's Democracy." *BBC News*, 2021. https://www.bbc.com/news/world-asia-india-57887300.

"BLASTPASS NSO Group IPhone Zero-Click, Zero-Day Exploit Captured in the Wild." *Citizenlab*, 2023. https://citizenlab.ca/2023/09/blastpass-nso-group-iphone-zero-click-zero-day-exploit-captured-in-the-wild/.

Boehm, Franziska. "A Comparison between US and EU Data Protection Legislation for Law Enforcement Purposes." *European Parliament*, 2015. https://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU(2015)536459_EN.pdf.

Burman, Anirudh. "The Withdrawal of the Proposed Data Protection Law Is a Pragmatic Move." *Carnegie India*, 2022. https://carnegieindia.org/2022/08/22/withdrawal-of-proposed-data-protection-law-is-pragmatic-move-pub-87710.

———. "Understanding India's New Data Protection Law." *Carnegie India*, 2023. https://carnegieindia.org/2023/10/03/understanding-india-s-new-data-protection-law-pub-90624.

"CASE OF ROMAN ZAKHAROV v. RUSSIA." *European Court of Human Rights*, 2015. https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-159324%22]}.

"CJEU Declares General Data Retention Unlawful in Tele2 Sverige." *CCDCOE*, 2016. https://ccdcoe.org/incyder-articles/cjeu-declares-general-data-retention-unlawful-in-tele2-sverige/.

"Demography of Europe – 2024 Edition." *Eurostat*, 2024. https://ec.europa.eu/eurostat/web/interactive-publications/demography-2024.

Dhillon, Amrit, and Michael Safi. "Indian Supreme Court Orders Inquiry into State's Use of Pegasus Spyware." *The Guardian*, 2021. https://www.theguardian.com/news/2021/oct/27/indian-supreme-court-orders-inquiry-into-states-use-of-pegasus-spyware.

"Discrimination in the European Union." *Eurostat*, n.d. https://europa.eu/eurobarometer/surveys/detail/2972.

"EU AI Act: First Regulation on Artificial Intelligence." *European Parliament*, 2023. https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.

"EU Charter of Fundamental Rights - Article 8." *Official Journal of the European Union C 303/17*, 2007. https://fra.europa.eu/en/eu-charter/article/8-protection-personal-data.

"EU Charter of Fundamental Rights- Article 7." *Official Journal of the European Union C 303/17*, 2007. https://fra.europa.eu/en/eu-charter/article/7-respect-private-and-family-life.

"EU: Landmark Digital Services Act Must Be Robustly Enforced to Protect Human Rights." *Amnesty International*, 2024. https://www.amnesty.org/en/latest/news/2024/02/eu-landmark-digital-services-act-must-be-robustly-enforced-to-protect-human-rights/.

Eurostat, ed. "Facts and Figures on the European Union." *European Union*, 2023. https://european-union.europa.eu/principles-countries-history/facts-and-figures-european-union_en.

"Fines / Penalties." *Intersoft Consulting*, n.d. https://gdpr-info.eu/issues/fines-penalties/.

"Forensic Methodology Report: How to Catch NSO Group's Pegasus." *Amnesty International*, 2021. https://www.amnesty.org/en/documents/doc10/4487/2021/en/.

Fung, Jenna Manhau, ed. "Bridging Divides and Navigating Digital Landscapes: A Study on Internet Access, Cybersecurity, and Sustainable Practices in Asia Pacific." *NetMission Academy Case Study Series*, 2024, 31.

GDPR. "Art. 22 - Automated Individual Decision-Making, Including Profiling." *Intersoft Consulting*, n.d. https://gdpr-info.eu/art-22-gdpr/.

George, Pameela. "India's Surveillance Landscape after the DPDPA." *IAPP*, 2025. https://iapp.org/news/a/india-s-surveillance-landscape-after-the-dpdpa.

Gerring, John. *"The Case Study: What It Is and What It Does", in Carles Boix, and Susan C. Stokes (Eds), The Oxford Handbook of Comparative Politics*. Oxford Handbooks, 2009. https://doi.org/10.1093/oxfordhb/9780199566020.003.0004.

"Global Internet Shutdowns: India." *Internet Society Pulse*, 2024. https://pulse.internetsociety.org/shutdowns.

"How Digital Rights Ireland Litigated Against the EU Data Retention Directive and Won." *Electronic Frontier Foundation*, 2014. https://doi.org/10.1016/j.clsr.2006.05.005.

"INDIA: ARRESTS, RAIDS TARGET CRITICS OF GOVERNMENT." *Amnesty International*, 2023. https://www.amnesty.org/en/documents/asa20/7303/2023/en/.

"India: Damning New Forensic Investigation Reveals Repeated Use of Pegasus Spyware to Target High-Profile Journalists." *Amnesty International*, 2023. https://www.amnesty.org/en/latest/news/2023/12/india-damning-new-forensic-investigation-reveals-repeated-use-of-pegasus-spyware-to-target-high-profile-journalists/.

"India: Dangerous Backsliding on Rights Activists, Critics Targeted; Growing Attacks on Muslims, Groups at Risk." *The Human Rights Watch*, 2022. https://www.hrw.org/news/2022/01/13/india-dangerous-backsliding-rights.

"India: Data Protection Bill Fosters State Surveillance." *Human Rights Watch*, 2022. https://www.hrw.org/news/2022/12/23/india-data-protection-bill-fosters-state-surveillance.

"India Explore All Countries," 2025. https://www.cia.gov/the-world-factbook/countries/india/#introduction.

"India: Spyware Use Violates Supreme Court Privacy Ruling." *Human Rights Watch (HRW)*, August 26, 2021. https://www.hrw.org/news/2021/08/26/india-spyware-use-violates-supreme-court-privacy-ruling.

"India Targeted High-Profile Journalists with Pegasus Spyware: Amnesty." *Aljazeera*, 2023. https://www.aljazeera.com/news/2023/12/28/india-targeted-high-profile-journalists-with-pegasus-spyware-amnesty?traffic_source=KeepReading.

"Indian Journalists Targeted by Israeli Spyware Again: What Do We Know?" *Aljazeera*, 2023. https://www.aljazeera.com/news/2023/12/28/indian-journalists-targeted-by-israeli-spyware-again-what-do-we-know.

"Information Technology Act, 2000," 2000. https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMjk4NzY=#:~:text=%5B9th%20June%2C%202000%5D%20An,communication%20and%20storage%20of%20information%2C.

International, Amnesty, and Citizen Lab. “India: Human Rights Defenders Targeted by a Coordinated Spyware Operation Summary Introduction.” *Amnesty International*, 2020. https://www.amnesty.org/en/latest/research/2020/06/india-human-rights-defenders-targeted-by-a-coordinated-spyware-operation/.

International, Amnesty, and Forbidden Stories. “About the Pegasus Project.” *Forbidden Stories*, n.d. https://forbiddenstories.org/about-the-pegasus-project/.

“Internet Usage in India.” *Statista*, 2024. https://www.statista.com/study/22628/internet-usage-in-india-statista-dossier/.

“Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors.” *Privacy Library*, 2017. https://nluwebsite.s3.ap-south-1.amazonaws.com/uploads/justice-ks-puttaswamy-ors-vs-union-of-india-ors-5.pdf.

Kakkar, Jhalak M., Nehmat Kaur, Sharngan Aravindakshan, Shashank Mohan, Shubhi Agarwal, Sravya Movva, Vrinda Bhandari, and Vasudev Devadasan. “The Surveillance Law Landscape in India and the Impact of Puttaswamy.” *National Law University Delhi Press*, 2023. https://ssrn.com/abstract=4624419.

Kirchgaessner, Stephanie. “Court Orders Maker of Pegasus Spyware to Hand over Code to WhatsApp.” *The Guardian*, 2024. https://www.theguardian.com/technology/2024/feb/29/pegasus-surveillance-code-whatsapp-meta-lawsuit-nso-group.

“Krzysztof Brejza v. Poland and 8 Other Applications.” *Amnesty International*, 2025, 11. https://www.amnesty.org/fr/wp-content/uploads/2025/02/EUR3790822025ENGLISH.pdf.

Law, Golden Data. “Commission v. Germany and the Independence of Supervisory Authorities.” *Medium*, 2019. https://medium.com/golden-data/commission-v-germany-and-the-independence-of-supervisory-authorities-d64dcb276b9a.

“Legal Framework of EU Data Protection.” *European Commission*, n.d. https://commission.europa.eu/law/law-topic/data-protection/legal-framework-eu-data-protection_en#:~:text=EU%20Member%20States%20have%20set,more%20than%20one%20Member%20State.

Lenka, Soumya. “Article 21 And Its Ever Expanding Scope.” *Legal Service India E-Journal*, n.d. https://www.legalserviceindia.com/legal/article-15808-article-21-and-its-ever-expanding-scope.html.

Masih, Niha, and Joanna Slater. “Further Evidence in Case against Indian Activists Accused of Terrorism Was Planted, New Report Says.” *The Washington Post*, 2021. https://www.washingtonpost.com/world/2021/04/20/india-bhima-koregaon-activists-report/.

Mesquita, Maria José Rangel de. “The Court of Justice of the European Union.” *Vox EU*, 2020, 451–67. https://doi.org/10.1163/9789004298712_027.

Mildebrath, Hendrik. “The CJEU Judgment in the Schrems II Case.” *European Parliamentary Research Service*, 2020. https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf.

“‘No Internet Means No Work, No Pay, No Food’ Internet Shutdowns Deny Access to Basic Rights in ‘Digital India.’” *Human Rights Watch*, 2023. https://www.hrw.org/report/2023/06/14/no-internet-means-no-work-no-pay-no-food/internet-shutdowns-deny-access-basic#:~:text=II.,by%20central%20and%20state%20governments.&text=These%20powers%20could%20be%20misused,or%20any%20form%20of%20oversight.

“NSO Group / Q Cyber Technologies.” *Citizen Lab*, 2019. https://citizenlab.ca/2019/10/nso-q-cyber-technologies-100-new-abuse-cases/.

O’Hara, Kieron, and Wendy Hall. “Four Internets : Data, Geopolitics, and the Governance of Cyberspace.” *Oxford University Press*, 2021. https://doi.org/10.1093/oso/9780197523681.001.0001.

Özkan, Ismail. “Data Protection Principles: The 7 Principles Of GDPR Explained.” *CyberPilot*, 2001.

Parsheera, Smriti, and Prateek Jha. “Cross-Border Data Access for Law Enforcement: What Are India’s Strategic Options?” *Carnegie India*, 2020. https://carnegieendowment.org/research/2020/11/cross-border-data-access-for-law-enforcement-what-are-indias-strategic-options?lang=en.

“PART III FUNDAMENTAL RIGHTS.” *The Constitution of India*, 1967. https://www.mea.gov.in/Images/pdf1/Part3.pdf.

Pírková, Eliška. “How the Digital Services Act Could Hack Big Tech’s Human Rights Problem.” *Access Now*, 2020. https://www.accessnow.org/eu-digital-services-act/.

Przeworski, Adam. *’ Is the Science of Comparative Politics Possible? ’, In Carles Boix, and Susan C. Stokes (Eds), The Oxford Handbook of Comparative Politics*. Oxford Handbooks, 2009. https://doi.org/10.1093/oxfordhb/9780199566020.003.0006.

Raikar, Sanat Pai, and Muzaffar Alam. “People of India.” *Britannica* 1 (2025): 1–6. https://doi.org/10.1109/ic2em59347.2023.10419441.

Roy, Annapurna. “How India Is Using the Internet.” *The Economic Times*, 2024. https://economictimes.indiatimes.com/tech/technology/how-india-is-using-the-internet/articleshow/108354854.cms?from=mdr.

Roy, Raktima, and Gabriela Zanfir-Fortuna. “The Digital Personal Data Protection Act of India Explained.” *Future of Privacy Forum*, August 15, 2023. https://fpf.org/blog/the-digital-personal-data-protection-act-of-india-explained/.

Sabha, Lok. “Report of the Joint Committee on the Personal Data Protection Bill,” 2021. https://prsindia.org/files/bills_acts/bills_parliament/2019/Joint_Committee_on_the_Personal_Data_Protection_Bill_2019.pdf.

“Section 69 in The Information Technology Act,” 2000. https://indiankanoon.org/doc/1439440/.

Shivshankar, V. “Privacy an Essential Aspect of Human Dignity, Says Supreme Court in Historic Ruling.” *The Wire*, 2017. https://thewire.in/law/supreme-court-right-to-privacy-verdict.

Singh, Kuldip. “People’S Union Of Civil Liberties ... vs Union Of India (Uoi),” 1996. https://indiankanoon.org/doc/31276692/.

Tejpal, Khyati, D.Y. Patil Vidyapeeth, Jayashree Patole, D.Y. Patil Vidyapeeth, Tanmay Ghugare, and D.Y. Patil Vidyapeeth. “Cybersecurity: Pressing Priority in India.” *Journal of Distance Education and E-Learning* 11, no. 2 (n.d.). https://tojdel.net/journals/tojdel/articles/v11i02b/v11i02b-42.pdf.

“The Court of Justice Declares the Data Retention Directive to Be Invalid.” *Court of Justice of the European Union*, 2014. https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf.

“THE DIGITAL PERSONAL DATA PROTECTION ACT,” 2023. https://indiankanoon.org/doc/3510545/.

“THE EU EPRIVACY REGULATION: WHAT IT IS AND WHAT TO EXPECT.” *USERCENTRICS Cookiebot*, 2024. https://www.cookiebot.com/en/eprivacy-regulation/#:~:text=Direct%20marketing%20communications%20under%20the,send%20such%20a%20marketing%20message.

“The European Data Protection Board.” *The European Data Protection Board (EDPB)*, 2022. https://www.edpb.europa.eu/about-edpb/who-we-are/european-data-protection-board_en#:~:text=Search%20on%20the%20EDPB%20web%20site:&text=It%20ensures%20that%20the%20General%20Data%20Protection,as%20the%20European%20Data%20Protection%20Supervisor%20(EDPS).

“THE INDIAN TELEGRAPH ACT Act No. 13,” 1885. https://dot.gov.in/sites/default/files/the_indian_telegraph_act_1985_pdf.pdf.

“The Information Technology Rules, 2011,” April 11, 2011.

"The NIS 2 Directive | Updates, Compliance." *NIS 2 Directive*, n.d. https://www.nis-2-directive.com/#:~:text=Stronger%20risk%20and%20incident%20management,of%20large%2Dscale%20cybersecurity%20incidents.

"Understanding the Risks of Digital IDs." *Immigrant Defense Project*, n.d. https://www.immigrantdefenseproject.org/wp-content/uploads/Digital-IDs-FAQ.pdf.

"Use of Entity Resolution in India: Shining a Light on How New Forms of Automation Can Deny People Access to Welfare." *Amnesty International*, 2024. https://www.amnesty.org/en/latest/research/2024/04/entity-resolution-in-indias-welfare-digitalization/.

"Weber and Saravia v. Germany: Case Analysis." *Global Freedom of Expression Columbia University*, n.d. https://globalfreedomofexpression.columbia.edu/cases/weber-saravia-v-germany/.

"What Is India's Caste System?" *BBC*, 2019. https://www.bbc.com/news/world-asia-india-35650616.

Wolford, Ben. "What Is GDPR, the EU's New Data Protection Law?" GDPR.EU, 2020. https://gdpr.eu/what-is-gdpr/.

ZAFFAR, HANAN, and JYOTI THAKUR. "How India's Government Uses Pegasus to Spy on Journalists." *Freedom Press*, 2024. https://ijnet.org/en/story/how-indias-government-uses-pegasus-spy-journalists.

Zalnieriute, Monika. "Data Transfers after Schrems II: The EU-US Disagreements over Data Privacy and National Security." *University of New South Wales* 55, no. 1 (2022). https://scholarship.law.vanderbilt.edu/vjtl/vol55/iss1/1/.

Zanfir-Fortuna, Raktima RoyGabriela, and Gabriela Zanfir-Fortuna. "THE DIGITAL PERSONAL DATA PROTECTION ACT OF INDIA, EXPLAINED." *The Future of Privacy Forum*, 2023. https://fpf.org/blog/the-digital-personal-data-protection-act-of-india-explained/.

Zetter, Kim. "Pegasus Spyware: How It Works and What It Collects." *Zero Day*, 2021. https://www.zetter-zeroday.com/pegasus-spyware-how-it-works-and/.