

Chapter 12

Illusion of Absolute Security: From Protection to Surveillance

Koyel Modak, Assistant Professor (Law), Swami Vivekananda University

Abstract

The promise of absolute security has become one of the most powerful narratives shaping contemporary governance, technology, and public imagination. In an age defined by cyber threats, terrorism, data breaches, and geopolitical instability, the demand for complete protection appears both rational and urgent. Yet, the idea of “absolute security” is conceptually flawed and politically consequential. This chapter argues that the pursuit of total protection gradually transforms protective mechanisms into pervasive systems of surveillance, thereby altering the relationship between the state, technology, and the individual.

The illusion lies in the belief that risk can be eliminated. Security, by its nature, is probabilistic. Technological systems are vulnerable, human actors are unpredictable, and threats continually evolve. Nonetheless, political discourse and corporate marketing often portray advanced surveillance technologies as capable of delivering near-total safety. This narrative fosters public consent for intrusive measures by framing privacy as an obstacle to security rather than as its complement.

This chapter critically examines how the shift from protection to surveillance occurs in three interconnected stages. First, it explores the securitization of fear, where exceptional threats are used to justify extraordinary measures. Second, it analyses the technological mediation of security, highlighting how data-driven governance prioritizes predictive control over reactive protection. Third, it interrogates the social consequences of normalized surveillance, including chilling effects on expression, behavioural conformity, and the marginalization of vulnerable groups through algorithmic bias.

Importantly, the chapter does not deny the legitimacy of security concerns. Rather, it challenges the assumption that more surveillance necessarily equates to greater safety. By tracing the historical and theoretical foundations of security discourse, it reveals how the pursuit of absolute protection can undermine democratic values, erode civil liberties, and concentrate power within opaque institutional and corporate structures. The paradox is that measures introduced to preserve freedom may gradually constrain it. The chapter ultimately advocates for a reframing of security as a balanced, accountable, and rights-respecting practice. Instead of striving for unattainable absolutes, policymakers must acknowledge the inevitability of risk and focus on proportionality, transparency, and oversight.

Keywords: *Absolute Security, Surveillance Society, Cyber Security, Data Governance, Digital Privacy, Securitization, State Power, Algorithmic Profiling, Biometric Identification, Risk Management, Civil Liberties, Technological Governance, Mass Data Collection; Predictive Policing; Democratic Accountability.*

Introduction

The contemporary world is increasingly shaped by narratives of security. Governments across the globe justify expansive technological infrastructures and legal frameworks in the name of protecting citizens from threats such as terrorism, cybercrime, and transnational insecurity. While these measures promise enhanced safety, they simultaneously generate complex concerns regarding privacy, civil liberties, and democratic accountability. We would examine the concept of the “illusion of absolute security,” arguing that the pursuit of total safety often results in the normalization of pervasive surveillance. This chapter draws an interdisciplinary perspective from law, political theory, and surveillance studies, it explores how security discourses legitimize monitoring practices that extend beyond their original purposes. It further highlights the role of digital technologies, biometric identification systems, algorithmic governance, and public-private partnerships in expanding the scope of surveillance. Despite an extensive body of literature on surveillance and privacy, a critical problem persists in understanding how contemporary societies internalize and normalize surveillance in everyday governance structures while maintaining the belief that such systems guarantee complete protection.²³⁸ This chapter addresses that problem by analysing the structural shift from protective security to surveillance-based governance. It concludes by proposing a rights-based framework that reconciles security objectives with democratic values through transparency, proportionality, and institutional accountability.

Security has historically been a central objective of the modern state. It has long been regarded as the fundamental responsibility of modern state. The legitimacy of political authority has often been justified by the promise of protecting citizens from violence, disorder, and external threats. In the contemporary era, however, the concept of security has expanded beyond traditional notions of military defence and policing. Governments now confront complex threats such as cyber warfare, terrorism, digital espionage, and organized transnational crime. These developments have encouraged the adoption of technologically advanced surveillance systems that monitor individuals, spaces, and communications.

In many contemporary societies, surveillance infrastructures are introduced under the promise of ensuring public safety. Digital monitoring tools, biometric databases, facial recognition systems, and algorithmic risk assessments are presented as necessary instruments to prevent harm. However, the mechanisms used to guarantee such protection as in mass data collection, biometric identification, predictive policing, and algorithmic monitoring have simultaneously expanded state surveillance. Yet these mechanisms also reshape the relationship between citizens and the state. The line between legitimate security practices and intrusive surveillance becomes increasingly blurred.

The notion of absolute security plays a significant role in this transformation. Political narratives frequently suggest that comprehensive monitoring and data analysis can eliminate risks and guarantee safety. However, such promises often obscure the social and legal consequences of surveillance expansion. The pursuit of total security may gradually normalize practices that undermine privacy, autonomy, and democratic oversight. This chapter examines the illusion of absolute security by

²³⁸ Julie E Cohen, ‘What Privacy Is For’ (2013) 126 *Harvard Law Review* 1904.

analysing how protective frameworks evolve into surveillance regimes.²³⁹ It also examines the paradox between the promise of absolute security and the gradual normalization of surveillance practices. It argues that the pursuit of complete security is inherently illusory because it requires intrusive monitoring that can erode civil liberties, privacy, and democratic accountability.²²⁵ It argues that modern security policies rely heavily on technological infrastructures that expand state power while creating new vulnerabilities and rights concerns. The chapter contributes to ongoing debates regarding the balance between security and liberty in the digital age. This chapter explores the illusion of absolute security by examining how contemporary security policies increasingly blur the line between protection and surveillance. It argues that while surveillance technologies can enhance security capabilities, their unchecked expansion risks transforming democratic societies into environments of continuous monitoring. The chapter concludes that democratic societies must critically reassess the narrative of absolute security and instead pursue a balanced approach that safeguards both safety and fundamental rights. Only by acknowledging the limits of security and reinforcing transparency, accountability, and rights-based regulation can societies prevent protection from gradually becoming pervasive surveillance.

Conceptual Foundations: Security, Surveillance and Governance

The relationship between security and governance has long been a subject of political and legal scholarship. Classical theories of the state emphasize that individuals consent to political authority in exchange for protection. According to this perspective, the state functions as a guarantor of security, ensuring order and stability within society.

Modern security governance, however, operates within a far more complex technological and institutional environment. Surveillance technologies have transformed the way states manage risks and monitor populations. Unlike traditional policing methods, digital surveillance allows authorities to collect and analyse vast amounts of information in real time.

Scholars of surveillance studies have observed that modern societies increasingly operate through systems of continuous observation and data collection. These systems are embedded not only within state institutions but also within everyday technologies such as smartphones, online platforms, and digital payment systems. As a result, surveillance has become an ordinary feature of social life rather than an exceptional practice.

The transformation of security governance reflects a broader shift from reactive to preventive strategies. Instead of responding to threats after they occur, modern security systems aim to predict and prevent potential risks. Predictive analytics, behavioural monitoring, and algorithmic profiling are increasingly used to identify patterns that may indicate future criminal or terrorist activity.

The expansion of surveillance is often justified by the argument that modern threats require sophisticated technological responses. Yet this reasoning also raises concerns about proportionality and

²³⁹ Bruce Schneier, *Beyond Fear: Thinking Sensibly About Security in an Uncertain World* (Springer 2003) 38. ²²⁵ Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA and the US Surveillance State* (Metropolitan Books 2014) 95.

accountability. When surveillance becomes pervasive, it alters the relationship between citizens and the state, shifting from trust-based governance to suspicion-based monitoring.

While preventive security offers certain advantages, it also raises important normative questions.²⁴⁰ The reliance on predictive technologies can result in extensive monitoring of individuals who have not committed any wrongdoing. This shift alters the traditional presumption of innocence and raises concerns about fairness, accountability, and discrimination.

The Expansion of Surveillance Technologies: Rise of Surveillance Society

Technological innovation has dramatically increased the capacity of both governments and private actors to monitor social behaviour. Advances in digital technology have significantly enhanced the capacity of governments and institutions to collect, store, and analyse personal data. Surveillance today is no longer limited to physical observation; it encompasses a vast array of digital processes that operate invisibly within everyday technologies. Contemporary surveillance infrastructures combine multiple forms of data collection, including biometric identification, location tracking, financial records, and digital communications.

Biometric technologies represent one of the most prominent developments in modern surveillance systems. Fingerprint databases, facial recognition tools, and iris-scanning technologies allow authorities to verify identities and track individuals across different contexts. While these technologies are often introduced to improve efficiency and security, they also create centralized repositories of sensitive personal information.

Another significant development is the rise of algorithmic governance. Security agencies increasingly rely on data analytics and artificial intelligence to identify suspicious patterns and predict potential risks. Predictive policing models analyse historical crime data to determine areas that require increased surveillance or policing presence.

The integration of surveillance technologies into everyday infrastructure further complicates the security landscape. Public spaces are now monitored through extensive networks of cameras, sensors, and digital tracking systems. At the same time, private technology companies collect enormous volumes of data through online platforms and digital services.

Moreover, surveillance is not solely conducted by governments. Private technology companies play an increasingly significant role in collecting and managing data. Their platforms generate vast datasets that can be accessed by state authorities through legal mandates or cooperative arrangements. This public-private collaboration further complicates questions of accountability and transparency.

The collaboration between public institutions and private corporations creates new forms of surveillance governance. Governments may access privately collected data for security purposes, while corporations develop technologies that shape surveillance practices. This relationship raises important questions regarding transparency, accountability, and regulatory oversight.

²⁴⁰ David Lyon, *Surveillance Society: Monitoring Everyday Life* (Open University Press 2001) 2.

Security Narratives and the Normalization of Surveillance

Public acceptance of surveillance policy measures often depends on the narratives used to justify them and emphasise fear and risk. Governments frequently invoke the language of emergency, threat, and protection to legitimize expanded monitoring powers. In times of crisis, citizens may be more willing to accept intrusive measures if they believe such actions are necessary to ensure safety.

This dynamic can lead to the gradual normalization of surveillance, as described as security narrative, where extraordinary measures become normalized through the language of protection. Temporary measures introduced during periods of crisis may become permanent features of governance. Over time, societies adapt to these practices, and surveillance becomes embedded within routine administrative functions and temporary emergency powers may become permanent features of governance.

The politics of fear can also influence legislative processes. Laws enacted in response to security crises often prioritize rapid action over careful consideration of rights implications. As a result, surveillance authorities may be granted broad powers with limited oversight.

The normalization process is reinforced by the perception that surveillance technologies are neutral and objective. However, these systems are designed and implemented within specific political and institutional contexts. Decisions regarding data collection, algorithmic criteria, and risk assessment often reflect broader social priorities and biases.

While such measures may initially target specific threats, their scope frequently expands. Surveillance technologies introduced for counter-terrorism purposes, for instance, may later be used for routine policing or administrative monitoring.²⁴¹

Moreover, the widespread use of digital technologies encourages individuals to voluntarily share personal information through social media platforms, mobile applications, and online services.²²⁸ This voluntary participation contributes to a culture in which surveillance becomes both institutional and self-imposed.

Data, Algorithms, and Predictive Security

One of the most significant developments in modern surveillance is the integration of algorithmic analysis into security systems. Predictive policing tools analyse historical crime data and behavioural patterns to anticipate potential incidents. Similarly, border security systems use risk-assessment algorithms to identify individuals considered suspicious.

Although these technologies promise greater efficiency, they also raise serious ethical and legal concerns. Algorithms rely on datasets that may reflect existing social biases. When such data are used to predict risk, they can reinforce discriminatory patterns in policing and law enforcement.

²⁴¹ Daniel J Solove, *Nothing to Hide: The False Trade-Off Between Privacy and Security* (Yale University Press 2011) 3.

²²⁸ Mireille Hildebrandt, *Smart Technologies and the End(s) of Law* (Edward Elgar 2015) 67.

Furthermore, algorithmic decision-making often lacks transparency. The criteria used to determine risk scores or threat assessments may not be publicly accessible. This opacity makes it difficult for individuals to challenge decisions that affect their rights.

Another concern relates to data centralization. Large-scale security databases combine information from multiple sources, including biometric records, financial transactions, travel histories, and online communications. The concentration of such sensitive data increases the risk of misuse, unauthorized access, or data breaches.

Specifically, there is limited research addressing how security narratives construct the perception that surveillance technologies can guarantee complete safety, thereby legitimizing the expansion of monitoring infrastructures. This chapter addresses that gap by examining the relationship between security discourse, technological governance, and the social acceptance of surveillance.

By analysing the illusion of absolute security, the chapter highlights how political narratives shape public perceptions of risk and protection. It also demonstrates that surveillance expansion is not solely driven by technological capability but also by the cultural and institutional belief that more monitoring inevitably leads to greater safety.

Legal and Human Rights Implications

The expansion of surveillance raises significant legal and ethical concerns. Privacy is widely recognized as a fundamental human right, essential for protecting individual autonomy, dignity, and freedom of expression.²⁴² Excessive monitoring can undermine these rights by creating an environment in which individuals feel constantly observed.

Legal frameworks attempt to balance security interests with individual rights through principles such as necessity, proportionality, and legality. Surveillance measures should therefore be justified by legitimate objectives and implemented only to the extent required to achieve those objectives.

However, contemporary surveillance infrastructures often operate on a scale that challenges traditional legal safeguards. Mass data collection and algorithmic decision-making can occur without meaningful public oversight or transparency. A key challenge lies in ensuring that surveillance measures remain proportionate and necessary. Broad or indiscriminate data collection may conflict with constitutional principles and human rights standards. Courts in various jurisdictions have increasingly scrutinized surveillance laws to determine whether they adequately protect individual liberties.

Another important concern relates to data security. Centralized databases containing biometric or behavioural information present significant risks if they are misused, hacked, or accessed without authorization. Data breaches involving sensitive personal information can have long-term consequences for individuals and institutions alike. Another significant issue concerns the role of private corporations in surveillance infrastructures.²³⁰ Technology companies that manage communication networks, cloud storage, and digital platforms possess vast quantities of user data.

²⁴² *Universal Declaration of Human Rights* (adopted 10 December 1948 UNGA Res 217 A(III)) art 12.

²³⁰ Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books 2019) 8.

When governments seek access to such data, questions arise regarding jurisdiction, consent, and the limits of corporate cooperation with state authorities.

Courts in various jurisdictions have increasingly recognized the importance of privacy protections in the digital age. Judicial decisions have emphasized that technological advancements must not erode the fundamental rights that underpin democratic societies.

The Illusion of Absolute Security

The pursuit of absolute security is inherently problematic because complete protection from all threats is unattainable. Societies are inherently dynamic and complex, and new forms of risk continuously emerge. Attempting to eliminate every potential threat would require an unrealistic level of control over social behaviour.

The belief in absolute security therefore functions as a political and technological myth. Surveillance systems can reduce certain risks, but they cannot eliminate uncertainty entirely.²⁴³ In fact, excessive reliance on surveillance may generate new vulnerabilities, including data misuse, institutional overreach, and technological dependence.

Furthermore, large-scale data collection can create information overload for security agencies. When authorities must analyse enormous datasets, identifying genuine threats becomes more difficult rather than easier. The pursuit of total security may therefore reduce rather than enhance effectiveness.

Recognizing the limits of security is essential for maintaining democratic values. Instead of striving for unattainable certainty, societies must focus on building resilient institutions that can respond effectively to emerging threats while respecting fundamental rights.

The illusion of absolute security therefore lies in the belief that technological surveillance can fully eliminate uncertainty. In reality, security strategies must acknowledge the limits of prediction and control.

Towards Balanced Security Governance and Rights-Based Security Framework

A balanced approach to security governance requires rethinking the relationship between protection and surveillance. Several policy recommendations can help address the challenges identified in this chapter.

1. Strengthening Legal Safeguards

Surveillance practices must operate within clear legal frameworks that define the scope and limitations of monitoring powers. Laws should specify the purposes for which data may be collected and ensure that surveillance activities are subject to judicial authorization.

²⁴³ Michel Foucault, *Discipline and Punish: The Birth of the Prison* (Alan Sheridan tr, Vintage Books 1995) 195.

2. Enhancing Institutional Oversight

Independent oversight bodies should be empowered to review surveillance practices and investigate potential abuses. Parliamentary committees, data protection authorities, and judicial institutions can play crucial roles in ensuring accountability.

3. Promoting Transparency

Transparency is essential for maintaining public trust. Governments should provide clear information regarding the technologies used for surveillance, the types of data collected, and the safeguards implemented to protect individual rights.

4. Implementing Privacy-by-Design

Technological systems should incorporate privacy protections at the design stage. Data minimization, encryption, and decentralized storage can reduce the risks associated with large-scale data collection.

Conclusion

The relationship between security and surveillance represents one of the defining challenges of the digital age. The pursuit of absolute security represents one of the most significant paradoxes of modern governance. While surveillance technologies promise protection against emerging threats, they also risk undermining the fundamental freedoms that democratic societies seek to protect.²⁴⁴

This chapter has argued that the belief in total security is largely illusory. Surveillance systems cannot eliminate uncertainty, and their unchecked expansion may create new vulnerabilities and rights concerns. By identifying a critical research gap in understanding how security narratives normalize surveillance, the chapter contributes to broader debates within legal and political scholarship. Ultimately, the challenge for contemporary societies lies in maintaining a delicate balance between safety and liberty. A sustainable approach to security requires recognizing that safety and liberty are not mutually exclusive but must be carefully balanced. Security policies must be grounded in principles of transparency, accountability, and respect for fundamental rights. Only by acknowledging the limits of surveillance and strengthening democratic safeguards can societies prevent the transformation of protective governance into pervasive monitoring. By reinforcing transparency, accountability, and rights-based regulation, societies can ensure that the pursuit of protection does not gradually transform into a regime of pervasive surveillance.

-----*****-----

²⁴⁴ David Lyon, *Surveillance Studies: An Overview* (Polity Press 2007) 14.