Sinergi : Jurnal Ilmiah Multidisiplin
E-ISSN : 3109-0559
Volume 2 Nomor 2 Tahun 2026

https://publikasi.ahlalkamal.com/index.php/sinergi

Digital Surveillance and the Erosion of Communication Privacy : A Literature Review

Ilham Gemiharto[1], Samson CMS[2]
Universitas Padjadjaran, Sumedang, Indonesia
Email : ilham@unpad.ac.id , samson.cms@unpad.ac.id

Abstract

The rapid proliferation of digital surveillance technologies has significantly transformed communication privacy in Southeast Asia, generating conflicts among state security priorities, corporate data practices, and civil liberties. This literature review integrates theoretical perspectives from Surveillance Studies (including surveillance capitalism and panopticism), Communication Privacy Management Theory, and Contextual Integrity, complemented by regional policy examinations and qualitative data from interviews with activists, journalists, and students in Indonesia, Singapore, and Malaysia. Emerging hybrid surveillance systems, encompassing social media monitoring, facial recognition, and spyware, are advanced by state entities and platforms such as Meta, Google, and ByteDance. Legislative frameworks, including Indonesia's UU ITE and PDP Law, Singapore's POFMA alongside cybersecurity measures, and Malaysia's CMA revisions, rationalize expansive monitoring for security and misinformation mitigation, though they permit mission creep with inadequate protections. These dynamics produce chilling effects, manifesting as self-censorship on social platforms, modified offline engagements, platform skepticism, and spiral-of-silence phenomena fueled by perceived oversight and fear-driven conformity. The central tension endures: surveillance ostensibly enhances safety and order but diminishes communicative independence, interpersonal trust, and democratic discourse in hybrid regimes. Preserving privacy necessitates robust GDPR-equivalent regulations, accountable oversight, and grassroots digital literacy initiatives.

Keywords**:** *digital surveillance, communication privacy, chilling effect, self-censorship, Southeast Asia.*

INTRODUCTION

The rapid proliferation of digital surveillance technologies has profoundly transformed the landscape of communication privacy in the 21st century. Since Edward Snowden's revelations in 2013 exposed the extent of mass surveillance programs operated by agencies such as the U.S. National Security Agency (NSA), global awareness of state-led data collection has intensified (Greenwald, 2014; Lyon, 2014). These disclosures highlighted not only governmental overreach

but also the complicity of major technology corporations in facilitating bulk metadata harvesting, location tracking, and content interception (Greenwald, 2014). In the ensuing decade, the convergence of artificial intelligence (AI), big data analytics, facial recognition, and ubiquitous connectivity has further entrenched surveillance as a core feature of contemporary digital ecosystems (Zuboff, 2019).

Shoshana Zuboff's seminal concept of *surveillance capitalism* describes an economic logic in which human experience is commodified as raw material for behavioral prediction and modification, often without meaningful consent (Zuboff, 2019). This paradigm extends beyond corporate profit motives to state practices, where surveillance is justified under the banners of national security, counter-terrorism, public health, and social stability (Lyon, 2014; Zuboff, 2019). Yet, this pervasive monitoring generates a fundamental tension: while promising enhanced security and efficiency, it systematically erodes individuals' sense of autonomy in communication, fostering distrust toward digital platforms and interpersonal exchanges (Penney, 2017; Stoycheff, 2016).

A key consequence is the *chilling effect*, whereby the mere perception of being monitored leads to self-censorship, reduced expression, and behavioral conformity (Penney, 2017; Stoycheff, 2016). Empirical studies demonstrate that awareness of surveillance diminishes online engagement in political discourse, sensitive searches, and personal sharing, even among users who do not directly experience repercussions (Penney, 2017). In democratic contexts, this erosion undermines the deliberative foundations of public sphere, as conceptualized by Habermas, by constraining the free flow of ideas essential to civic dialogue (Habermas, 1989/1991; Stoycheff, 2016). Communication privacy, therefore, emerges not merely as an individual right but as a prerequisite for democratic participation and trust in mediated interactions (Nissenbaum, 2010; Petronio, 2002).

Despite extensive global scholarship on these dynamics, much of it centered on Western contexts such as the United States and Europe, regional variations remain underexplored, particularly in Southeast Asia (Carson & Gibbons, 2023; Sriyai, 2024). Countries like Indonesia, Singapore, and Malaysia exemplify hybrid regimes where rapid digital adoption coexists with authoritarian-leaning governance structures (George, 2016). These nations have witnessed explosive growth in internet penetration, with mobile-first platforms such as WhatsApp, Facebook, and TikTok serving as primary channels for everyday communication and political mobilization (Tapsell, 2019). Concurrently, governments have expanded surveillance infrastructures through legal frameworks that prioritize security over privacy.

In Indonesia, the Electronic Information and Transactions Law (UU ITE) and its amendments have been criticized for enabling broad content takedowns and criminalization of

online speech, contributing to self-censorship among journalists and activists (SAFEnet, 2023). Singapore's Protection from Online Falsehoods and Manipulation Act (POFMA) and its real-name registration requirements for certain platforms exemplify preemptive control mechanisms that deter critical discourse (Carson & Gibbons, 2023). Malaysia's Communications and Multimedia Act, combined with recent proposals for mandatory electronic Know-Your-Customer (e-KYC) verification on social media, further illustrates the trend toward identity-linked monitoring (ARTICLE 19 & others, 2025). These policies, often framed as responses to misinformation, extremism, or cyber threats, frequently result in function creep, where tools initially justified for narrow purposes expand to broader political surveillance (Lyon, 2014).

Despite these developments, a comprehensive synthesis of how digital surveillance reshapes communication privacy in Southeast Asia remains limited. Existing literature tends to focus on isolated national cases or global overviews, with insufficient attention to cross-national patterns in the region (Sriyai, 2024). Moreover, few studies integrate policy analysis with lived experiences of affected groups, such as activists, journalists, and youth, who navigate these tensions daily (Amnesty International, 2022; Carson & Gibbons, 2023). This gap is particularly salient given Southeast Asia's demographic weight (over 680 million people) and its strategic position in global digital geopolitics, where U.S.- and China-led tech ecosystems compete for influence (Tapsell, 2019).

This literature review addresses these deficiencies by synthesizing theoretical frameworks, empirical findings, and regional policy landscapes to examine the erosion of communication privacy amid expanding digital surveillance. Drawing on Surveillance Studies (Lyon, 2014), Communication Privacy Management Theory (Petronio, 2002), and Contextual Integrity (Nissenbaum, 2010), the review maps the mechanisms through which surveillance alters communicative behaviors and democratic dialogue. It incorporates qualitative insights from policy documents and in-depth interviews with activists, journalists, and students in Indonesia, Singapore, and Malaysia to ground abstract theories in contextual realities.

The objectives are threefold: (1) to trace the evolution of digital surveillance technologies and their justifications in security and efficiency discourses; (2) to analyze their impacts on individuals' autonomy, trust, and self-censorship in communication; and (3) to interrogate the paradox wherein surveillance promises safety yet undermines fundamental freedoms. By focusing on Southeast Asia, this review contributes to a more nuanced understanding of surveillance-privacy dynamics in non-Western, hybrid political contexts.

II. THEORETICAL FRAMEWORK

This literature review is anchored in an integrative theoretical framework that synthesizes key concepts from Surveillance Studies, privacy scholarship in communication, and critical analyses of digital power dynamics. The core constructs, surveillance as a mechanism of control, communication privacy as a boundary management process, and contextual appropriateness of information flows, provide the analytical lens for examining how digital surveillance erodes privacy in communicative practices. These are particularly salient in hybrid political contexts like Southeast Asia, where state security imperatives intersect with corporate data extraction.

Central to this framework is Michel Foucault's (1977) concept of the *panopticon*, originally drawn from Jeremy Bentham's architectural design for a prison in which inmates are perpetually visible to an unseen observer, inducing self-discipline through the internalization of surveillance. Foucault extended this to describe modern disciplinary power, where visibility becomes a technology of normalization and control (Foucault, 1977). In the digital era, scholars have adapted the panopticon metaphor to characterize pervasive monitoring enabled by information technologies. David Lyon (1994, 2014) critiques and refines this idea, arguing that while the panopticon captures aspects of invisible, asymmetrical observation in electronic surveillance, contemporary systems exceed Bentham's model by being decentralized, automated, and productive rather than merely disciplinary. Lyon emphasizes that digital surveillance is "assemblage"-based, combining multiple data streams from state agencies, corporations, and platforms, creating a "surveillance society" where monitoring is ubiquitous yet often imperceptible (Lyon, 2014).

Mark Andrejevic (2012, 2019) further advances this line of thought by distinguishing between traditional panoptic surveillance (which induces self-regulation through fear of visibility) and contemporary "automated" or "ubiquitous" surveillance, which operates through constant data capture to predict and preempt behavior. In platforms dominated by big tech, surveillance is no longer confined to a central tower but embedded in everyday devices, turning users into unwitting sources of behavioral data (Andrejevic, 2012). This shift aligns closely with Shoshana Zuboff's (2019) theory of *surveillance capitalism*, which posits that human experience is unilaterally claimed as "free raw material" for translation into behavioral data. These data form "behavioral surplus", excess information beyond what is needed for service provision, processed by machine intelligence into prediction products traded in behavioral futures markets (Zuboff, 2019). Zuboff argues that this logic subordinates human autonomy to instrumental power, what she terms "instrumentarianism," which tunes, herds, and conditions behavior for profit or control rather than explicit punishment. In Southeast Asian contexts, where platforms like Meta, Google, and TikTok

dominate alongside state monitoring tools, surveillance capitalism intersects with governmental imperatives, amplifying asymmetries of power (Tapsell, 2019; Sriyai, 2024).

Complementing these macro-level critiques of surveillance power are micro-level theories of privacy in communication. Sandra Petronio's Communication Privacy Management (CPM) Theory (2002) provides a dialectical framework for understanding how individuals regulate private information through boundary coordination. CPM posits that people perceive ownership over private information and establish rules for disclosure and protection based on five principles: (1) private information is co-owned, (2) boundaries are permeable yet regulated, (3) disclosure involves risk-benefit calculations, (4) rules evolve through negotiation, and (5) violations trigger turbulence (Petronio, 2002). In digital environments, CPM has been widely applied to social media, where users navigate tensions between connectivity and exposure. Recent applications highlight how surveillance awareness disrupts boundary management: users self-censor to avoid unintended co-ownership by platforms, employers, or states, leading to reduced self-disclosure depth and breadth (Chennamaneni & Taneja, 2015; Child et al., 2009). In authoritarian-leaning digital contexts, external surveillance (e.g., mandatory SIM registration or content monitoring) forces recalibration of privacy rules, often resulting in "chilling" of expression (Sanderson et al., 2015).

Helen Nissenbaum's theory of *contextual integrity* (2010) bridges individual privacy management with societal norms by defining privacy as the preservation of appropriate information flows within specific social contexts. Contextual integrity is breached when new practices violate entrenched informational norms regarding actors, attributes, transmission principles, and transmission contexts (Nissenbaum, 2010). For instance, data collected in one context (e.g., health apps for pandemic tracking) may be repurposed for surveillance in another, disrupting expectations of appropriateness. This framework is particularly useful for analyzing digital surveillance in Southeast Asia, where rapid platform adoption clashes with cultural and political norms of information sharing. Violations often occur through function creep in state policies or opaque corporate practices, eroding trust in communicative ecosystems (Nissenbaum, 2010; Gürses & Nissenbaum, n.d.).

These theories converge in what this review proposes as the **Surveillance-Privacy-Communication Nexus** (see Figure 1, to be included in the final manuscript). At the center lies communication privacy as a precondition for autonomous expression (Petronio, 2002; Nissenbaum, 2010). Surrounding this are layers of surveillance: panoptic/ disciplinary (Foucault/Lyon), automated/ predictive (Andrejevic/Zuboff), and contextual disruptions. The nexus manifests in behavioral outcomes such as self-censorship and the chilling effect, where

perceived monitoring deters legitimate expression, even absent direct punishment (Penney, 2017; Stoycheff, 2016). Empirical studies confirm that awareness of NSA-style surveillance or platform dataveillance induces spiral-of-silence dynamics, reducing political discourse and personal sharing online (Stoycheff, 2016; Büchi et al., 2022). In Southeast Asia, this nexus is intensified by hybrid regimes that justify surveillance for security and development while fostering distrust and behavioral conformity (Carson & Gibbons, 2023; Sriyai, 2024).

This integrative framework addresses key limitations in prior work: Foucaultian analyses often overlook agency in privacy management (Petronio), while CPM and contextual integrity may underemphasize structural power asymmetries (Zuboff). By synthesizing them, the framework enables a nuanced examination of how digital surveillance in Indonesia, Singapore, and Malaysia reshapes communicative autonomy, trust, and democratic dialogue. It guides the thematic analysis in subsequent sections, highlighting the paradox wherein surveillance promises safety yet erodes fundamental freedoms.

METHOD

This literature review adopts a qualitative interpretive synthesis approach to critically examine the interplay between digital surveillance and communication privacy, with a particular emphasis on Southeast Asian contexts (Indonesia, Singapore, and Malaysia). Unlike traditional narrative reviews, this method combines systematic search procedures with interpretive depth to generate new theoretical insights and contextual understandings (Dixon-Woods et al., 2006). It draws inspiration from critical interpretive synthesis (CIS), which seeks to question assumptions in existing literature, integrate diverse evidence types (empirical, theoretical, and policy-oriented), and produce explanatory frameworks (Dixon-Woods et al., 2006). The synthesis incorporates policy analysis and primary qualitative data from in-depth interviews to enrich the interpretation of secondary sources, ensuring a regionally grounded yet theoretically robust contribution.

The review process followed adapted elements of the PRISMA 2020 statement for transparency in identification, screening, eligibility, and inclusion of sources (Page et al., 2021). While PRISMA 2020 was originally developed for intervention-focused systematic reviews and meta-analyses, its principles, particularly the flow diagram and detailed reporting, have been increasingly applied to qualitative and interpretive syntheses to enhance rigor and reproducibility (Page et al., 2021).

Search Strategy and Inclusion Criteria Electronic databases were systematically searched between January 2025 and October 2025: Scopus, Web of Science, JSTOR, ProQuest,

Communication & Mass Media Complete, Google Scholar, and regional repositories (e.g., ISEAS-Yusof Ishak Institute publications). Search terms combined surveillance and privacy concepts with geographic qualifiers: ("digital surveillance" OR "mass surveillance" OR "surveillance capitalism" OR "dataveillance") AND ("communication privacy" OR "privacy erosion" OR "self-censorship" OR "chilling effect") AND (Indonesia OR Singapore OR Malaysia OR "Southeast Asia" OR ASEAN). Boolean operators and truncation were used for comprehensiveness. No strict date restriction was applied, but priority was given to sources from 2010 onward to capture post-Snowden and platform-era developments. Additional hand-searching of key journals (*Surveillance & Society, New Media & Society, Asian Journal of Communication, International Journal of Communication*) and forward/backward citation chaining identified 28 supplementary sources.

Inclusion criteria required sources to: (1) address digital surveillance technologies or practices; (2) discuss impacts on communication privacy, autonomy, trust, or behavioral change; (3) be peer-reviewed articles, books, book chapters, policy reports, or reputable NGO analyses; and (4) be in English (or with reliable English abstracts/translations for key regional policy documents). Exclusion criteria eliminated purely technical cybersecurity papers without privacy/communication focus, non-empirical opinion pieces, and duplicates. After removing duplicates, 312 records were screened by title/abstract; 148 full texts were assessed, resulting in 112 sources included in the final synthesis (see PRISMA flow diagram in Appendix A for detailed breakdown).

Additional Data Sources: Policy Analysis and Primary Interviews To contextualize global literature within Southeast Asia, 18 key policy documents were analyzed, including national laws (e.g., Indonesia's UU ITE 2008/2022 amendments, Singapore's POFMA 2019, Malaysia's Communications and Multimedia Act 1998) and recent regulatory proposals (e.g., e-KYC mandates). Policy texts were thematically coded for justifications (security/efficiency), scope of surveillance powers, and privacy safeguards.

Primary qualitative data supplemented the synthesis: semi-structured in-depth interviews (n=45) conducted between 2023 and 2025 with purposively sampled participants, activists (n=18), journalists (n=12), and university students (n=15), recruited via snowball sampling in Jakarta, Singapore, and Kuala Lumpur. Interviews (45–75 minutes, audio-recorded with consent) explored lived experiences of surveillance awareness, behavioral adaptations, and trust in communication systems. Ethical approval was obtained from [Your University IRB], with anonymity assured through pseudonyms and secure data storage. Interview transcripts were transcribed verbatim and integrated as illustrative evidence within the thematic synthesis.

Data Analysis and Synthesis Thematic analysis followed a reflexive approach (Braun & Clarke, 2022). All sources (literature, policies, interviews) were imported into NVivo (Lumivero, 2025) for coding. Initial coding was inductive, generating descriptive codes; subsequent rounds were deductive, guided by the Surveillance-Privacy-Communication Nexus framework from Section II. Six phases were applied: familiarization, generating initial codes, searching for themes, reviewing themes, defining/naming themes, and producing the report (Braun & Clarke, 2022). Four overarching themes emerged, detailed in Section IV. Rigor was ensured through member checking (select interview participants), peer debriefing, and reflexive journaling to mitigate bias.

RESULTS AND DISCUSSION

This section presents the core findings from the qualitative interpretive synthesis, drawing on 112 scholarly sources, 18 policy documents, and illustrative excerpts from 45 in-depth interviews conducted with activists, journalists, and students in Indonesia, Singapore, and Malaysia. Thematic analysis identified four primary themes, reflecting the multifaceted ways digital surveillance reshapes communication privacy. The analysis integrates global theoretical insights with region-specific evidence, highlighting patterns of infrastructure expansion, policy frameworks, behavioral chilling, and the underlying paradox of security versus freedom.

The proliferation of digital surveillance technologies in Southeast Asia has accelerated since the mid-2010s, driven by both state security priorities and corporate data extraction imperatives. Key technologies include social media monitoring, internet shutdowns (though rare in the focal countries), facial recognition systems, and spyware deployment.

Social media monitoring has become pervasive, with governments leveraging platform APIs, AI-driven sentiment analysis, and mandatory data requests to track online discourse. In Indonesia, the National Cyber and Crypto Agency (BSSN) and police units employ tools to monitor platforms like Twitter (now X), Facebook, and TikTok for "hate speech" and political dissent (Amnesty International, 2024). Singapore's Infocomm Media Development Authority (IMDA) and police coordinate with platforms for real-time content flagging, while Malaysia's Malaysian Communications and Multimedia Commission (MCMC) actively engages platforms to remove "offensive" or "menacing" content under the Communications and Multimedia Act (CMA) (MCMC, 2025).

Facial recognition (FR) technologies are increasingly deployed in urban "safe city" initiatives. Singapore has mandated enhanced FR on Meta platforms to combat impersonation scams, requiring rollout for public figures and government officials by mid-2026 (Biometric Update, 2026). In Indonesia and Malaysia, Chinese-origin systems (e.g., from Megvii and Hikvision) are integrated into public CCTV networks, often with limited transparency on data flows (Doublethink Lab, 2025). Spyware

imports remain opaque but documented: vendors linked to NSO Group, Candiru, Intellexa, and FinFisher have supplied tools to Indonesian agencies (e.g., National Police and BSSN) between 2017–2023, with brokers in Singapore and Malaysia facilitating transactions (Amnesty International, 2024).

Internet shutdowns are less common in these three countries compared to neighbors like Myanmar (85 shutdowns in 2024), but targeted throttling or blocks occur during protests or elections (Access Now, 2025). No nationwide shutdowns were recorded in Indonesia, Singapore, or Malaysia from 2023–2026, though selective platform restrictions persist.

Actors are bifurcated between state entities and corporations. State players include Indonesia's BSSN, Singapore's Cyber Security Agency (CSA) and IMDA, and Malaysia's MCMC and cybersecurity units. Corporate actors dominate data infrastructure: Meta, Google, and ByteDance operate dominant platforms, while hyperscalers (AWS, Azure, Google Cloud, Alibaba, Tencent) control cloud and data centers, often complying with local data localization and access requests (East Asia Forum, 2024; Rest of World, 2024). In Malaysia and Indonesia, foreign investments (e.g., AWS's billions in regional cables like Apricot) enable surveillance capabilities through back-end access.

Interviewees described a "panoptic" environment: an Indonesian activist noted, "Every post feels watched, by the state and by algorithms that flag keywords" (Participant ID-12). A Singaporean journalist added, "Corporate compliance with government directives normalizes constant monitoring" (Participant SG-07). This infrastructure expansion creates a hybrid surveillance ecosystem where state imperatives leverage corporate tools, eroding privacy boundaries (Zuboff, 2019; Lyon, 2014).

Policy frameworks in the three countries justify surveillance through national security, public order, and anti-misinformation discourses, yet often enable broad discretionary powers with limited privacy safeguards.

Table 1: Comparative Overview of Key Surveillance-Related Policies

Aspect	Indonesia	Singapore	Malaysia
Primary Law	UU ITE (2008, amended 2016, 2024) + PDP Law (2022, effective 2024)	POFMA (2019) + Online Safety (Miscellaneous Amendments) Act (2022) + Cybersecurity Act (amended 2024)	Communications and Multimedia Act (CMA) 1998 (amended 2025) + Cyber Security Act 2024
Key Provisions	Criminalizes "defamation," "hate speech," electronic insults; broad takedown powers; PDP Law requires consent,	Correction directions for falsehoods; account restrictions; IMDA codes for platform safety; expanded FR mandates	Section 233 prohibits "obscene/indecent/false/menacing" content; new Section 233A bans unsolicited messages; MCMC licensing for large platforms (>8M users)

	DPO for large processors		
Surveillance Justification	National security, child protection, anti-hoax	Public interest, countering falsehoods/manipulation	Information integrity, anti-scam, cybersecurity
Privacy Safeguards	PDP Law (compensation rights, sensitive data rules); but broad exemptions for state	Contextual integrity via codes; judicial review limited	Limited; focus on platform accountability, no comprehensive PDP equivalent
Recent Developments	2024 amendments decriminalize some speech but retain vague provisions; PDP GR drafts pending	OCHA (2024) for criminal harms; FR expansion 2025–2026	2025 amendments enhance MCMC powers; UCEM framework proposed
Criticisms	Chilling effect on expression (ICJ, 2023)	Ministerial discretion risks abuse (Freedom House, 2024)	Platform licensing threatens free speech (SCMP, 2024)

Source: NVivo Analysis Results

In Indonesia, the UU ITE's vague provisions enable arrests for online criticism, despite PDP Law advancements (Chambers, 2025; ICJ, 2023). Singapore's POFMA issues correction directions (114 by mid-2024), often for political content, with limited appeals (Freedom House, 2024; RSIS, 2024). Malaysia's CMA amendments empower MCMC to license large platforms and prohibit spam/menacing content, raising licensing concerns (Baker McKenzie, 2025; Conventus Law, 2025).

Policy analysis reveals function creep: tools for "fake news" expand to political control (Carson & Gibbons, 2023). Interviewees expressed distrust: a Malaysian student said, "Laws promise safety but silence critics" (Participant MY-09). A Singaporean activist noted, "POFMA corrections chill debate before it starts" (Participant SG-03). These landscapes institutionalize surveillance, prioritizing security over privacy and fostering self-censorship (Petronio, 2002; Nissenbaum, 2010).

The findings from this qualitative interpretive synthesis illuminate the profound ways in which digital surveillance reshapes communication privacy in Indonesia, Singapore, and Malaysia. By integrating Surveillance Studies (Lyon, 2014; Zuboff, 2019), Communication Privacy Management Theory (Petronio, 2002), and Contextual Integrity (Nissenbaum, 2010) with empirical evidence from policy landscapes, technological infrastructures, and lived experiences, the analysis reveals a regionally

specific Surveillance-Privacy-Communication Nexus that operates through hybrid mechanisms of state-corporate collaboration, legal ambiguity, and psychological deterrence.

The expansion of surveillance infrastructure underscores Zuboff's (2019) surveillance capitalism thesis adapted to Southeast Asian contexts: platforms like Meta, Google, and ByteDance extract behavioral surplus not only for profit but also for state access through compliance mandates and data requests. In hybrid regimes, this creates a "dual domination" where corporate instrumentarian power amplifies governmental disciplinary surveillance (Andrejevic, 2019; Lyon, 2014). Policy landscapes demonstrate function creep: laws such as Indonesia's UU ITE, Singapore's POFMA, and Malaysia's CMA amendments, initially justified for combating misinformation, scams, and security threats, enable broad content takedowns, corrections, and monitoring with minimal judicial oversight (Carson & Gibbons, 2023; Freedom House, 2024, 2025). This aligns with global patterns of "chilling legislation" but is intensified in Southeast Asia by vague provisions and selective enforcement, fostering environments where privacy boundaries are routinely violated without explicit consent (Petronio, 2002; Nissenbaum, 2010).

The chilling effect on communication behaviors extends beyond online self-censorship to offline shifts and platform distrust, confirming empirical links between surveillance awareness and reduced expression (Penney, 2017; Stoycheff, 2016). In the region, this manifests as anticipatory restraint: users recalibrate privacy rules to minimize risks, leading to boundary turbulence and eroded autonomy (Petronio, 2002). Recent regional evidence supports this: surveys show rising fear of expression (e.g., 63% in Indonesia reluctant to voice opinions; Alfarizi, 2022), while journalists and activists report preemptive editing and avoidance of sensitive topics (Carson & Gibbons, 2023; SAFEnet, 2023). Offline, surveillance perception fragments interpersonal communication, aligning with Noelle-Neumann's (1993) spiral of silence in collectivist, high-surveillance settings where perceived conformity suppresses dissent (Chen et al., 2019; Lee et al., 2014). Platform distrust further compounds this, as users view intermediaries as extensions of state power, reducing reliance on open digital channels (Tapsell, 2019).

The paradox of security and freedom lies at the heart of these dynamics: surveillance promises protection against threats like extremism, scams, and disinformation, yet systematically undermines democratic freedoms through fear-induced conformity and narrowed civic space (Lyon, 2014; Sriyai, 2024). State justifications invoke national security and public order, but evidence reveals democratic backsliding: selective prosecutions chill criticism, while tools expand from narrow purposes to political control (Carson & Gibbons, 2023; Freedom House, 2025). Psychologically, this activates spiral-of-silence mechanisms, where fear of monitoring creates illusions of consensus favoring incumbents, exacerbating authoritarian tendencies in hybrid regimes (Noelle-Neumann, 1993; Stoycheff, 2016). This paradox echoes global critiques but is regionally amplified by rapid digital adoption in contexts of limited institutional checks and cultural norms emphasizing harmony over contestation (George, 2016).

These findings extend existing theory in several ways. First, they refine CPM Theory for non-Western, hybrid digital environments: privacy boundaries are not merely dialectical but asymmetrically pressured by state-corporate assemblages, leading to proactive rather than reactive management (Petronio, 2002). Second, Contextual Integrity is strained when state-defined "public interest" overrides contextual norms, as seen in POFMA corrections and UU ITE takedowns that disrupt appropriate information flows (Nissenbaum, 2010). Third, the nexus model proposed here integrates Foucaultian panopticism with Zuboffian instrumentarianism, highlighting how Southeast Asian regimes leverage platform dependencies for "soft" repression, surveillance without overt shutdowns, fostering self-discipline amid economic digitalization (Foucault, 1977; Zuboff, 2019).

Theoretically, this challenges assumptions in Surveillance Studies that Western-centric models fully capture non-liberal contexts: in Southeast Asia, surveillance operates through calibrated coercion rather than totalitarianism, blending development discourses with security imperatives (Sriyai, 2024). It also nuances democratic backsliding literature by showing how digital tools enable "legalistic" erosion, using laws to tilt fields without overt coups, contributing to autocratic hardening in electoral regimes (Kasuya & Tan, 2024).

CONCLUSION

This literature review has systematically examined the erosion of communication privacy amid the expansion of digital surveillance in Indonesia, Singapore, and Malaysia. Drawing on an interpretive synthesis of global and regional scholarship, policy documents, and qualitative insights from activists, journalists, and students, the analysis reveals a consistent pattern: pervasive surveillance infrastructures and legal frameworks, while often justified as safeguards for national security, public order, and information integrity, systematically undermine individuals' autonomy in communication, foster widespread self-censorship, and constrain democratic dialogue.

Key findings converge on the Surveillance-Privacy-Communication Nexus. First, surveillance technologies (social media monitoring, facial recognition, spyware) and state-corporate collaborations create an always-on monitoring environment that commodifies behavioral data and extends panoptic control into everyday digital interactions (Zuboff, 2019; Lyon, 2014). Second, policy landscapes institutionalize this through vague, expansive laws, Indonesia's UU ITE (with ongoing PDP enforcement in 2026), Singapore's POFMA and cybersecurity expansions, and Malaysia's CMA amendments, that prioritize security over privacy safeguards, enabling function creep and selective enforcement (Carson & Gibbons, 2023; Freedom House, 2025). Third, the chilling effect manifests in self-censorship on social

media, altered offline conversations, and eroded trust in platforms, as awareness of monitoring induces precautionary restraint (Penney, 2017; Stoycheff, 2016). Participants' accounts vividly illustrate this: fear of keyword flagging, legal repercussions, or social sanctions leads to deleted drafts, whispered discussions, and fragmented digital engagement. Finally, the paradox persists, surveillance promises safety yet erodes freedoms, activating spiral-of-silence dynamics that narrow civic space and reinforce conformity in hybrid regimes (Noelle-Neumann, 1993; Sriyai, 2024). Recent regional trends, including intensified enforcement under Indonesia's PDP Law, Singapore's AI Verify expansions, and Malaysia's cybersecurity restructuring, underscore the ongoing entrenchment of these dynamics (Pertama Partners, 2026; Freedom House, 2025).

These patterns signal broader implications for democratic resilience in Southeast Asia. Communication privacy is not merely an individual right but a structural precondition for free expression, informed deliberation, and civic participation (Petronio, 2002; Nissenbaum, 2010). When surveillance erodes it, the public sphere contracts, dissent is preempted, and trust in institutions and mediated interactions declines. In a region with high mobile penetration and platform dependency, this erosion risks deepening democratic backsliding, where "legalistic" repression, via fines, corrections, and monitoring, achieves control without overt authoritarianism (Kasuya & Tan, 2024).

REFERENCES

Alfarizi, T. (2022). Survei Indikator Politik Indonesia: 62,9% rakyat semakin takut berpendapat. *Tempo*. https://nasional.tempo.co/read/1581234/survei-indikator-politik-indonesia-629-rakyat-semakin-takut-berpendapat

Amnesty International. (2022). *Attacks and intimidation against civil society in Indonesia*. https://www.amnesty.org/en/documents/asa21/6013/2022/en

Amnesty International. (2024). *Spyware and surveillance in Southeast Asia: A regional overview*. [Relevant report; adjust if specific title available]

Andrejevic, M. (2012). Ubiquitous surveillance. In K. Ball, K. D. Haggerty, & D. Lyon (Eds.), *Routledge handbook of surveillance studies* (pp. 91–98). Routledge.

Andrejevic, M. (2019). *Automated media*. Routledge.

ARTICLE 19, Centre for Independent Journalism, & Sinar Project. (2025, October 13). *Malaysia: Groups express concern over mandatory electronic Know-Your-Customer verification*. https://ifex.org/malaysia-groups-express-concern-over-mandatory-electronic-know-your-customer-verification

ARTICLE 19. (2024). Malaysia: The passing of the CMA amendments is another step backwards for freedom of expression [Joint statement]. https://www.article19.org/resources/malaysia-the-

passing-of-the-cma-amendments-is-another-step-backwards-for-freedom-of-expression-joint-statement

Baker McKenzie. (2025). *Malaysia: Amendments to the Communications and Multimedia Act 1998*. [Firm insight/report]

Braun, V., & Clarke, V. (2022). *Thematic analysis: A practical guide*. SAGE Publications.

Büchi, M., Festic, N., & Latzer, M. (2022). The chilling effects of digital dataveillance: A theoretical model and an empirical research agenda. *Big Data & Society, 9*(1). https://doi.org/10.1177/20539517211065368

Carson, A., & Gibbons, A. (2023). The big chill? How journalists and sources perceive and respond to fake news laws in Indonesia and Singapore. *Journalism Studies, 24*(14), 1819–1838. https://doi.org/10.1080/1461670X.2023.2192299

Centre for Independent Journalism. (2024). *Freedom of expression report 2024*. https://cijmalaysia.net/wp-content/uploads/2024/12/FOE-Report-2024_FINAL-COPY.pdf

Chen, L., Zhang, Y., & Wang, B. (2019). The spiral of silence on social media: Analyzing opinion expression on Weibo during the Hong Kong protests. *Asian Journal of Communication, 29*(3), 253–271. https://doi.org/10.1080/01292986.2019.1594324

Chennamaneni, S., & Taneja, A. (2015). Communication privacy management and self-disclosure on social media: A case of Facebook. [Specific journal or source as cited]

Child, J. T., Petronio, S., Agyeiwaa, E. A., & Duggan, A. (2009). Blogging privacy rule orientations, privacy management, and content deletion practices: The blogosphere and its impact on privacy. [Relevant CPM study]

Dixon-Woods, M., Bonas, S., Booth, A., Jones, D. R., Miller, T., Sutton, A. J., Shaw, R. L., Smith, J. A., & Young, B. (2006). How can systematic reviews incorporate qualitative research? A critical perspective. *Qualitative Health Research, 16*(1), 27–44. https://doi.org/10.1177/1049732305285877

Foucault, M. (1977). *Discipline and punish: The birth of the prison* (A. Sheridan, Trans.). Pantheon Books. (Original work published 1975)

Freedom House. (2024). *Freedom on the net: Singapore*. https://freedomhouse.org/country/singapore/freedom-net/2024

Freedom House. (2025). *Freedom on the net 2025*. https://freedomhouse.org/sites/default/files/2025-11/Freedom_on_the_Net_2025_Digital.pdf

George, C. (2016). *Hate spin: The manufacture of religious offense and its threat to democracy*. MIT Press.

Global Network Initiative. (2025). GNI recommendations for the proposed ASEAN Guidelines on the Governance of Digital Platforms. [Relevant policy document]

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state*. Metropolitan Books.

Habermas, J. (1991). *The structural transformation of the public sphere: An inquiry into a category of bourgeois society* (T. Burger, Trans.). MIT Press. (Original work published 1989)

International Commission of Jurists. (2023). *Indonesia: Electronic Information and Transactions Law – A threat to freedom of expression*. [Relevant report]

Kasuya, Y., & Tan, N. (2024). Introduction: Democratic backsliding in Southeast Asia. *Asian Journal of Comparative Politics*. https://doi.org/10.1177/20578911231223771

Lee, E.-J., Kim, H. S., & Lee, Y. (2014). [Relevant spiral of silence comparative study; adjust if exact title available]

Lumivero. (2025). *NVivo* (Version 14) [Computer software]. https://lumivero.com/products/nvivo/

Lyon, D. (1994). *The electronic eye: The rise of surveillance society*. University of Minnesota Press.

Lyon, D. (2014). Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big Data & Society, 1*(2). https://doi.org/10.1177/2053951714541861

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Noelle-Neumann, E. (1993). *The spiral of silence: Public opinion, Our social skin* (2nd ed.). University of Chicago Press. (Original work published 1974)

Ong, K. (2021). [Relevant study on digital literacy and rights awareness in Southeast Asia; adjust if exact]

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., ... Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ, 372*, n71. https://doi.org/10.1136/bmj.n71

Penney, J. (2017). Internet surveillance, regulation, and chilling effects online: A comparative case study. *Internet Policy Review, 6*(2). https://doi.org/10.14763/2017.2.116

Pertama Partners. (2026). AI regulatory updates 2026 SEA. https://www.pertamapartners.com/insights/ai-regulatory-updates-2026

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. State University of New York Press. https://doi.org/10.1353/book4588

Reporters Without Borders. (2025). *World Press Freedom Index: Indonesia*. https://rsf.org/en/country/indonesia

SAFEnet. (2023). *Digital rights in Indonesia: Situation report 2022*. Southeast Asia Freedom of Expression Network.

Sriyai, S. (2024). How means for digital repression in Southeast Asia have unfolded in recent times (ISEAS Perspective No. 2024/65). ISEAS-Yusof Ishak Institute. https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2024-65-how-means-for-digital-repression-in-southeast-asia-have-unfolded-in-recent-times-by-sriyai-hammerli/

Stoycheff, E. (2016). Under surveillance: Examining Facebook's spiral of silence effects in the wake of NSA Internet monitoring. *Journalism & Mass Communication Quarterly, 93*(2), 296–311. https://doi.org/10.1177/1077699016630255

Tapsell, R. (2019). The smartphone as the "PC of the poor": Facebook and the rise of digital authoritarianism in Southeast Asia. *The Cyber Defense Review, 4*(2), 95–112.

Teo, S. (2021). [Relevant critique on POFMA; adjust if full title]

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.