World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

ENCRYPTION UNDER SIEGE: BALANCING NATIONAL SECURITY, LAW ENFORCEMENT ACCESS, AND CIVIL LIBERTIES IN THE DIGITAL AGE

Victor Mensah *

Tagliatela College of Engineering, Cybersecurity and Networks, University of New Haven, United States of America.
* Corresponding Author

World Journal of Advanced Research and Reviews, 2026, 32(02), 1362–1371

Publication history: Received on 10 October 2026; revised on 16 November 2026; accepted on 18 November 2026

Article DOI: https://doi.org/10.30574/wjarr.2026.32.2.2823

Copyright © 2026 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution License 4.0

ABSTRACT

The rapid expansion of encrypted communication has placed governments, technology companies, and civil society on a collision course. Encryption protects the confidentiality, integrity, and authenticity of digital communication, yet the same properties that shield ordinary users from criminals and hostile states also shield criminals and hostile actors from lawful investigation. This paper examines the policy, legal, and ethical terrain surrounding encryption, government access, and civil liberties. It situates the debate within the broader "going dark" discourse, reviews the technical and legal mechanisms governments use to seek access to encrypted data including mandated backdoors, lawful hacking, and data retention regimes and examines the well-documented risks of deliberately weakened security. Two case studies, the 2016 Apple v. FBI dispute and the 2013 Snowden revelations, illustrate how these abstract tensions play out in practice. The paper then situates encryption policy within a wider ecosystem of digital rights, extending the analysis to algorithmic content moderation and platform governance, which raise parallel questions about transparency, due process, and the limits of private power. Comparative analysis of the United States, the United Kingdom, and the European Union highlights how differing legal traditions produce different balances between security and privacy. The paper concludes with policy recommendations emphasizing judicial oversight, technical safeguards, and international harmonization as the most viable path toward reconciling security imperatives with fundamental rights.

Keywords: Encryption Policy, Government Surveillance, Digital Privacy and Civil Liberties, Lawful Access to Encrypted Communications, Digital Rights and Platform Governance

1 INTRODUCTION

Encryption sits at the intersection of two values that most democratic societies claim to hold simultaneously: the right of individuals to communicate privately, and the responsibility of the state to protect its citizens from crime and violence. As more of everyday life banking, healthcare, political organizing, journalism, and intimate conversation has migrated onto encrypted digital platforms, the stakes of this tension have grown accordingly. Encryption is no longer a niche cryptographic tool used by governments and specialists; it is the default architecture of modern communication (Koops, 2023).

This paper argues that encryption policy cannot be understood in isolation. It is embedded in a broader ecosystem of digital governance that includes surveillance law, cross-border evidence-sharing regimes, and the increasingly

consequential power that private platforms exercise over public discourse through algorithmic moderation. Treating encryption purely as a technical problem, or purely as a law-enforcement problem, obscures the civil-liberties dimension that runs through all of these debates: the right to private communication, the right to due process, and the right to be free from unaccountable surveillance, whether conducted by a government agency or a private platform's algorithm.

The paper proceeds in three parts. First, it establishes the technical and rights-based foundations of encryption and situates the "going dark" debate within legal scholarship. Second, it examines two defining case studies Apple v. FBI (2016) and the Snowden disclosures (2013) that crystallized public understanding of the trade-offs involved. Third, it broadens the lens to compare international regulatory approaches and to connect encryption policy with the adjacent field of algorithmic content moderation, before closing with policy recommendations.

2 ENCRYPTION: CONCEPT AND RIGHTS-BASED FRAMING

Encryption is the process of converting information into an unreadable format that can only be reversed with the correct cryptographic key. It underpins messaging applications such as WhatsApp and Signal, online banking, e-commerce, government communications, and cloud storage. Its value rests on three properties that security professionals treat as foundational.

Table 1: Core Properties of Encryption and Representative Applications

Property	What It Ensures	Representative Application
Confidentiality	Only authorized parties can read the content of a message	End-to-end encrypted messaging (Signal, WhatsApp)
Integrity	Data has not been altered in transit or storage	Software update verification, financial transactions
Authentication	Verifies the identity of users, devices, or systems	TLS certificates, banking logins, secure email
Non-repudiation	Prevents a party from denying it sent or received data	Digitally signed contracts and legal documents
Availability of secure defaults	Protects users who take no additional action	Full-disk encryption enabled by default on smartphones

Beyond its technical function, encryption increasingly carries normative weight as a rights-protecting mechanism rather than a mere convenience. Koops (2023) frames encryption as a way of preventing unlawful access rather than simply resisting lawful access a distinction that matters because it reframes strong encryption not as an obstacle to the state, but as a safeguard consistent with the state's own obligation to protect its citizens' data from criminals, foreign intelligence services, and corporate overreach. Privacy itself is recognized as a fundamental human right under Article 12 of the Universal Declaration of Human Rights, encompassing control over personal information, freedom from surveillance, and protection from unauthorized access. Civil liberties scholarship treats these protections as inseparable from due process and freedom of expression: without confidential communication, journalists cannot protect sources, dissidents cannot organize safely, and ordinary citizens cannot exercise autonomy over their private lives.

3 CIVIL LIBERTIES AND PRIVACY IN THE DIGITAL AGE

European jurisprudence has been particularly influential in articulating privacy as an evolving right that must adapt to new surveillance technologies. van der Sloot (2018) traces how the European Court of Human Rights has moved toward a "non-domination" principle, under which the mere possibility of arbitrary interference with private communications not just proven misuse can constitute a rights violation. This is a significant conceptual shift: it means that broad surveillance architectures can be unlawful even before any specific abuse occurs, simply because they create the structural conditions for domination.

Borgesius and Steenbruggen (2019) extend this analysis to the right to confidentiality of communications in Europe, arguing that this right protects not only content but also metadata the who, when, and how long of digital communication that intelligence agencies have historically treated as less sensitive than content itself. This distinction matters directly for encryption policy, because many surveillance regimes that cannot break encryption instead pursue bulk metadata collection as a workaround, a pattern examined further in Section 5.

Civil liberties concerns are not confined to state actors. As communication has moved onto private platforms, questions of due process, transparency, and freedom of expression increasingly implicate the design choices of technology companies themselves a theme this paper returns to in Section 9 when it connects encryption policy to algorithmic content moderation.

4 GOVERNMENT SECURITY NEEDS AND THE "GOING DARK" DEBATE

Law enforcement and intelligence agencies argue that the widespread adoption of strong, default encryption has caused them to "go dark" losing access to communications and stored data that they were previously able to obtain with a warrant. Koops and Kosta (2018) situate this concern within the longer history of the "crypto wars," tracing how governments have repeatedly sought policy tools to counteract the spread of unbreakable encryption, from export controls in the 1990s to contemporary backdoor mandates and lawful-hacking proposals.

The going-dark debate is best understood as occupying a spectrum rather than a binary choice between total access and total secrecy. At one end, governments could mandate that all encrypted systems retain a decryption capability; at the other, systems could be designed so that not even the manufacturer holds a key (zero-knowledge or "no-access" design). Figure 1 illustrates this spectrum and the intermediate mechanisms data retention laws, lawful hacking, and default end-to-end encryption that occupy the space between these extremes.

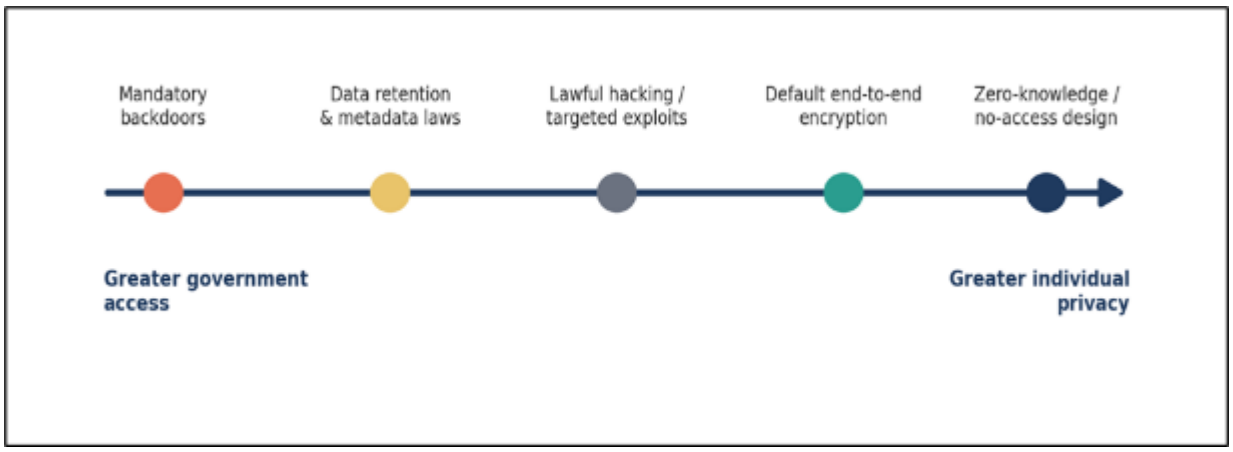


Figure 1: The Security–Privacy Spectrum in Encryption Policy.

Each point on this spectrum carries distinct trade-offs. Mandatory backdoors offer the broadest and most immediate access but, as discussed in Section 5, introduce systemic vulnerabilities. Lawful hacking preserves encryption's integrity for the general population while allowing targeted access in specific investigations, but it is resource-intensive and raises its own oversight concerns. Default end-to-end encryption maximizes user protection but can genuinely impede time-sensitive investigations. No single point on the spectrum is costless, which is precisely why the debate has persisted for three decades without resolution.

5 LEGAL AND TECHNICAL MECHANISMS FOR GOVERNMENT ACCESS

Where legislatures and courts have sought to preserve law-enforcement access to digital evidence, several distinct mechanisms have emerged, each with a different risk profile. Kerr and Schneier (2018) provide an influential taxonomy of "encryption workarounds" that avoid directly breaking cryptographic algorithms, instead targeting the endpoints, the key-management process, or the human operators of encrypted systems.

Abelson et al. (2015), in the widely cited "Keys Under Doormats" report, argue that any mechanism guaranteeing government access inevitably expands the attack surface available to criminals and hostile states: a key that can be retrieved by a court order can, in principle, be retrieved by anyone who compromises the same storage or escrow system. This technical argument has proven durable precisely because it does not depend on political sympathies it is a claim about the mathematics and engineering of secure systems, not about the trustworthiness of any particular government.

Figure 2 summarizes how these mechanisms relate to one another as alternative pathways a government may pursue when it seeks access to encrypted data, along with the central risk-benefit trade-off that runs through all of them.

Table 2: Comparison of Government Access Mechanisms

Mechanism	How It Works	Primary Risk / Limitation
Mandated backdoor	Legally requires a built-in decryption capability in products or services	Creates a systemic vulnerability exploitable by any party who discovers it (Abelson et al., 2015)
Lawful hacking	Government exploits existing software vulnerabilities under judicial authorization	Resource-intensive; incentivizes agencies to withhold vulnerability disclosures (Liguori, 2020)
Data retention / metadata law	Compels providers to store communications metadata for a fixed period	Reveals sensitive relational and behavioral patterns even without message content (Borgesius & Steenbruggen, 2019)
Legal compulsion (e.g., All Writs Act, CLOUD Act)	Courts order a company to assist in accessing a specific device or account	Cross-border enforcement is legally contested and inconsistent (Svantesson, 2021)
Encryption workaround (endpoint access)	Targets the device or the user rather than the cryptographic algorithm itself	Still requires exploiting a vulnerability or compelling cooperation (Kerr & Schneier, 2018)

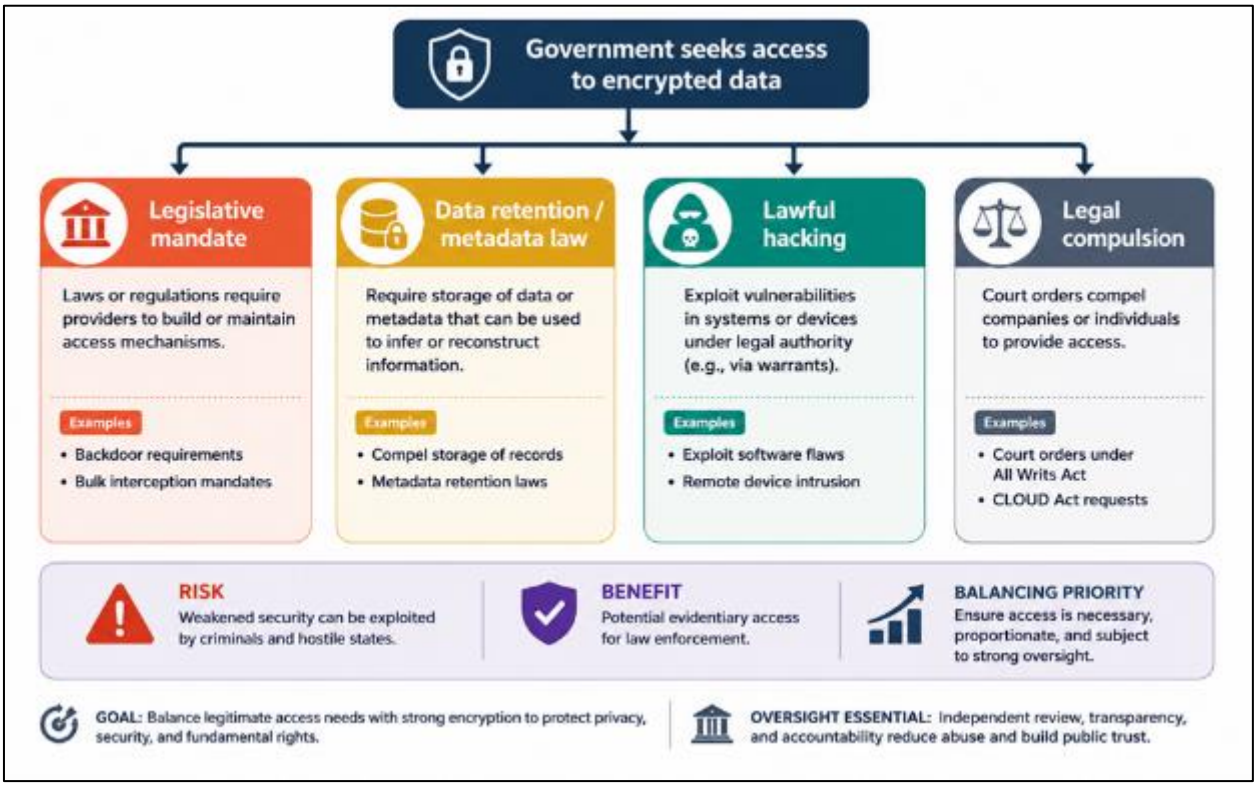


Figure 2: Pathways Governments Use to Seek Access to Encrypted Data.

Liguori (2020) argues that lawful hacking, despite its costs, represents the most defensible compromise currently available: it preserves strong encryption as a general-purpose protection while allowing targeted, judicially supervised access in individual cases. Critics counter that lawful hacking still requires agencies to stockpile knowledge of vulnerabilities rather than disclosing them for patching leaving the same vulnerabilities available to be discovered independently by criminal or foreign actors, an ongoing dilemma within intelligence agencies' vulnerability equities processes.

6 CASE STUDY I: APPLE V. FBI (2016)

In December 2015, an attack in San Bernardino, California left fourteen people dead. One of the attackers, Syed Farook, owned a work-issued iPhone 5C that was locked and encrypted, with a security feature that would erase its contents after too many failed password attempts. Unable to bypass this protection, the FBI obtained a court order compelling

Apple to build custom software that would disable the auto-erase feature and allow unlimited password attempts a tool that Apple, and much of the security community, characterized as a backdoor.

Apple refused to comply, arguing publicly that creating such software would establish a dangerous precedent: a tool built once could be demanded again, and its existence would itself become a target for theft or misuse. The company's resistance rested on the same technical logic articulated by Abelson et al. (2015) that a capability built for one legitimate investigation cannot be selectively limited to that investigation alone.

The FBI pursued the matter in court under the All Writs Act of 1789, a statute that predates modern computing by more than two centuries, illustrating a recurring theme in this literature: legal frameworks for compelling technical assistance were rarely designed with encryption in mind (Rudesill, 2015, on the broader problem of governing emerging surveillance capacities through ambiguous or outdated legal authority). Before the case was resolved on the merits, the FBI announced it had accessed the phone using a third-party tool, reportedly supplied by the Israeli firm Cellebrite, and the case was dropped.

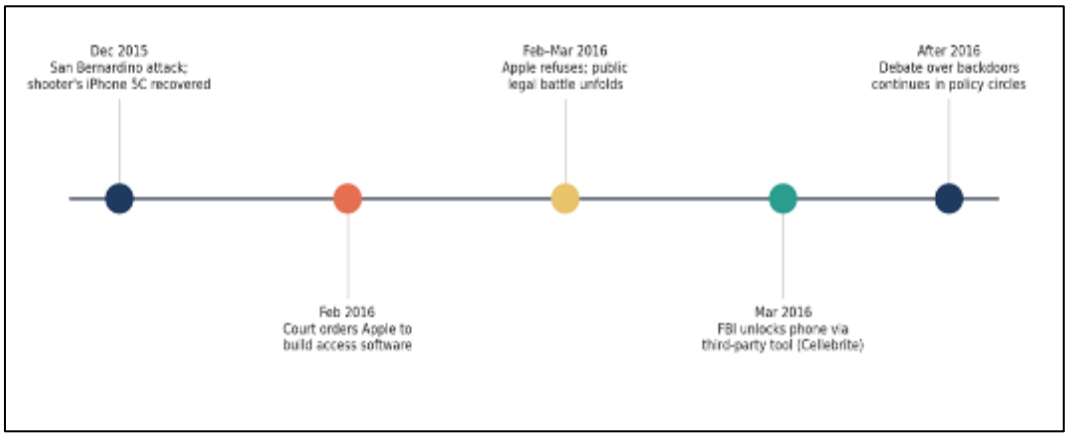


Figure 3: Timeline of the Apple v. FBI San Bernardino Case (2015–2016).

Although the case never produced binding precedent, it functioned as a public referendum on the going-dark debate, sharpening popular understanding of concepts that had previously been confined to specialist literature: the difference between a targeted exploit and a systemic backdoor, and the tension between a single investigation's urgency and encryption's broader protective function.

7 CASE STUDY II: NSA MASS SURVEILLANCE AND THE SNOWDEN REVELATIONS

In 2013, former NSA contractor Edward Snowden disclosed a large volume of classified material revealing the scale of U.S. government surveillance programs, including the PRISM program, which provided access to data held by major technology companies, and bulk telephone metadata collection affecting millions of people both domestically and abroad. Unlike the Apple v. FBI case, which centered on a single device, the Snowden disclosures concerned surveillance conducted at a systemic, population-wide scale, implicating not only American citizens but foreign governments and allied leaders.

Table 3: Contrasting Positions in the Surveillance-versus-Privacy Debate

Surveillance Advocates Argue	Privacy Advocates Argue
Bulk collection helps identify terrorist and criminal networks before an attack occurs	Mass collection is disproportionate and unconstitutional absent individualized suspicion
National security interests can outweigh individual privacy claims in narrow circumstances	Unchecked surveillance erodes public trust in government and democratic institutions
Targeted surveillance under warrant is a legitimate and long-standing law-enforcement tool	Even the possibility of arbitrary interference can constitute a rights violation (van der Sloot, 2018)
Metadata is less sensitive than content and can be collected with lighter oversight	Metadata reveals intimate relational patterns and deserves confidentiality protection (Borgesius & Steenbruggen, 2019)

The disclosures produced concrete policy consequences, including the USA FREEDOM Act's reforms to bulk metadata collection, and accelerated the technology industry's adoption of default end-to-end encryption as a competitive and trust-building response. They also intensified an ethical debate that scholars had already begun to formalize: is mass, population-wide data collection ever justified by security benefits, or does the accumulation of that capability itself constitute an unacceptable risk of abuse, regardless of how it is currently being used?

Taken together, the Apple v. FBI and Snowden episodes illustrate two different but related failure modes in the security-privacy balance: the first concerns whether a single company can be compelled to build a tool that undermines its own product's security; the second concerns whether the state can justify collecting data about an entire population in the name of security that only a small fraction of that population poses any risk to.

8 COMPARATIVE AND CROSS-BORDER POLICY APPROACHES

Encryption and surveillance policy differ substantially across jurisdictions, reflecting distinct legal traditions and institutional structures. In the United States, the PATRIOT Act (2001) and the FISA Amendments Act (2008) expanded surveillance authorities, while the proposed EARN IT Act has sought to condition certain legal protections for technology companies on cooperation with law enforcement regarding encrypted content, particularly around child-protection concerns. Cross-border data requests are further complicated by jurisdictional friction, which Svantesson (2021) identifies as one of the central unresolved problems in international law enforcement: a request for electronic evidence often implicates the laws of the country where the data is stored, the country where the crime occurred, and the country where the company is headquartered, each potentially imposing conflicting obligations.

Table 4: Comparative Overview of Encryption and Surveillance Policy Approaches

Jurisdiction	Primary Legal Instruments	General Orientation
United States	PATRIOT Act (2001); FISA Amendments Act (2008); EARN IT Act (proposed); All Writs Act (1789)	Expands surveillance authority; relies on courts and legislation to compel cooperation case-by-case
United Kingdom	Investigatory Powers Act framework; Covert Human Intelligence Sources (Criminal Conduct) Act 2021	Distinguishes technical vs. legal backdoors; broad authorization of covert investigative conduct
European Union	General Data Protection Regulation; European Convention on Human Rights jurisprudence	Emphasizes communications confidentiality and a non-domination privacy standard
Germany / France	National implementations alongside EU law	Support targeted lawful-access measures despite strong EU-level privacy norms

The United Kingdom occupies a distinctive position, having enacted investigatory powers legislation that explicitly contemplates lawful-access obligations. McDermott (2025) distinguishes between "technical backdoors" built directly into software and "legal backdoors" created through compulsion orders that require a company to decrypt data on request without necessarily altering the underlying system design a distinction that matters because the two approaches carry very different security implications even when their practical effect on privacy is similar. Scott (2022) separately examines the UK's Covert Human Intelligence Sources (Criminal Conduct) Act 2021, which illustrates how surveillance-adjacent legal authority can expand well beyond encryption itself, into the authorization of covert conduct by intelligence sources.

The European Union, by contrast, has generally emphasized privacy protection through the General Data Protection Regulation and a robust body of European Court of Human Rights jurisprudence, although individual member states, including France and Germany, have at times supported lawful-access obligations that sit in tension with the EU's broader rights framework. Rudesill (2015) offers a cautionary note applicable across all these systems: much of the underlying legal authority for surveillance and data-access programs has historically been interpreted through classified or otherwise inaccessible legal opinions, a phenomenon he terms "secret law," which complicates any comparative assessment because the public text of a statute may not reflect how it is actually applied.

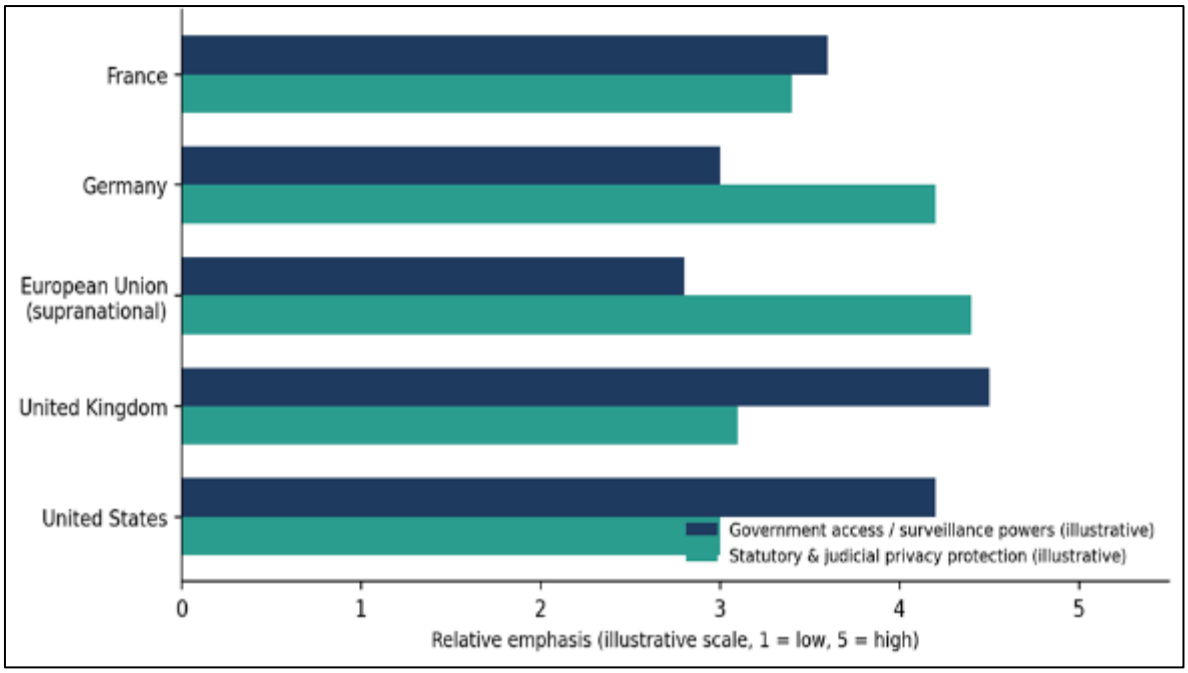


Figure 4: Illustrative Comparison of Surveillance Powers and Privacy Protections Across Jurisdictions Discussed in the Literature.

The comparison in Figure 4 is illustrative rather than a precise index; it is intended to visualize the qualitative pattern described in the literature reviewed above, where common-law jurisdictions have generally emphasized broader law-enforcement access mechanisms, while EU-level jurisprudence has emphasized communications confidentiality as a structural right, even as individual member states diverge from that emphasis in practice.

9 BEYOND ENCRYPTION: PLATFORM GOVERNANCE AND ALGORITHMIC CONTENT MODERATION

Encryption policy does not exhaust the civil-liberties questions raised by digital communication. As platforms have become central venues for public discourse, their internal governance how they moderate content, rank information, and enforce rules raises parallel questions about transparency, due process, and the limits of private power, even though no government surveillance is directly involved. Suzor (2018) frames this as a problem of "digital constitutionalism": platforms exercise governance functions traditionally associated with states, yet without the constitutional constraints, such as rule of law and due process, that legitimize state authority.

Gorwa, Binns, and Katzenbach (2020) describe how content moderation has shifted from manual human review toward automated, algorithmic systems operating at a scale no human workforce could match, raising technical and political challenges around consistency, appeals, and error rates. Cobbe (2021) extends this analysis to the concept of algorithmic censorship, arguing that automated moderation systems can suppress lawful speech in ways that are difficult to detect or contest precisely because their decision logic is opaque even to the platforms that deploy them. Cotter (2021) documents a related phenomenon she terms "black box gaslighting": when users suspect their content has been suppressed ("shadowbanned") but platforms deny that any such mechanism exists, users are left unable to verify or challenge decisions that materially affect their reach and livelihood.

Caplan and Gillespie (2020) show how these governance structures extend into the platform economy itself, describing "tiered governance" arrangements in which enforcement severity and demonetization risk vary by creator status, again largely outside public accountability mechanisms. Quintais, Appelman, and Fahy (2022) examine how platforms' own terms of service have become a vehicle, however imperfect, for importing fundamental-rights standards into content moderation practice, while Helberger (2019) raises a related concern about the democratic role of algorithmic news recommenders, which shape the informational environment citizens rely on to form political judgments without being subject to the editorial accountability traditionally expected of publishers.

Table 5: Mechanisms and Civil-Liberties Concerns in Algorithmic Content Moderation

Mechanism	Function	Associated Concern
Automated content classifiers	Flag or remove content at scale using machine learning	Opaque decision logic and inconsistent enforcement (Gorwa et al., 2020)
Visibility reduction ("shadowbanning")	Limits reach of content without formal removal	Undermines a user's ability to know or contest the decision (Cotter, 2021)
Tiered enforcement / demonetization	Applies different consequences based on creator status or history	Uneven accountability across the platform economy (Caplan & Gillespie, 2020)
Terms-of-service adjudication	Platform interprets and applies its own rules to user conduct	Limited due process compared to public legal systems (Suzor, 2018)
Algorithmic recommendation / ranking	Determines what content users see and in what order	Shapes democratic discourse without editorial accountability (Helberger, 2019)

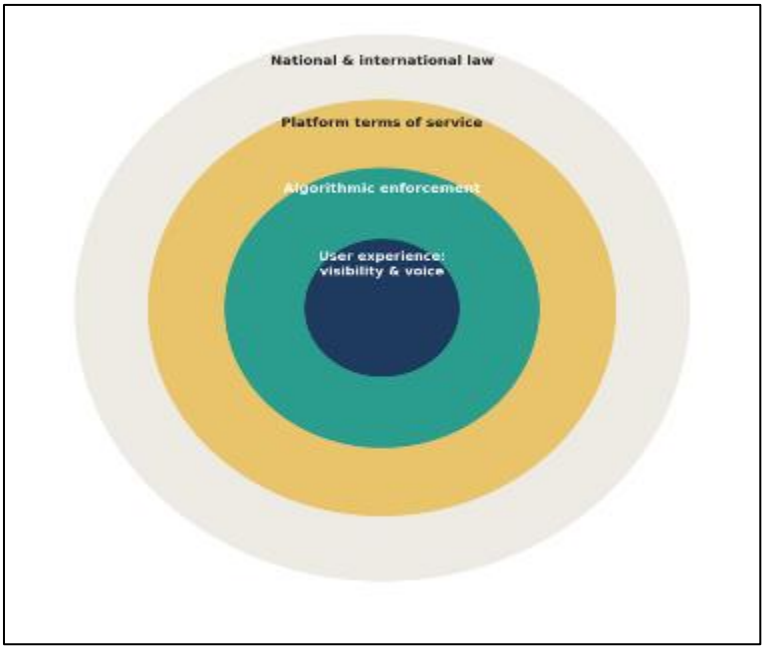


Figure 5: Layers of Platform Governance (Digital Constitutionalism).

The parallel between encryption policy and platform governance is instructive. In both domains, a technology originally designed for a narrow technical purpose securing a message, or filtering spam has become the substrate on which much larger civil-liberties questions are contested. And in both domains, the central reform proposals converge on similar principles: transparency about how a system works, meaningful avenues for individuals to contest decisions made about them, and independent oversight that does not rely solely on the good faith of the institution being overseen.

10 ETHICAL TENSIONS AND POLICY RECOMMENDATIONS

The literature reviewed in this paper points toward several converging conclusions, even though scholars disagree sharply about specific policy instruments. First, mandated backdoors carry a well-documented systemic security cost that is difficult to confine to any single, legitimate use case (Abelson et al., 2015); policymakers should treat this technical finding as a serious constraint on backdoor mandates rather than as one contested opinion among many. Second, targeted mechanisms such as lawful hacking, conducted under judicial authorization and subject to independent oversight, appear to offer a more defensible middle path than blanket backdoor requirements, though they require their own safeguards against overuse and vulnerability hoarding (Liguori, 2020; Kerr & Schneier, 2018).

Third, cross-border legal frameworks require greater harmonization. The jurisdictional friction identified by Svantesson (2021) means that companies and users currently face inconsistent, sometimes contradictory obligations depending on where data is stored and where an investigation originates; clearer international agreements, with built-

in human-rights safeguards, would reduce both over-compliance and under-compliance with legitimate law-enforcement requests. Fourth, legal authority for surveillance and data-access programs should be publicly available in a form the public can evaluate, addressing Rudesill's (2015) "secret law" concern, since a policy debate conducted without access to the actual legal standards in force is necessarily incomplete.

Finally, given the structural parallels identified in Section 9, encryption policy should not be developed in isolation from platform governance reform. Both domains would benefit from independent oversight bodies, meaningful transparency reporting, and accessible mechanisms for individuals to contest decisions whether those decisions are made by a government agency seeking access to a device, or by an algorithm determining what content a user is permitted to see.

11 CONCLUSION

Encryption policy is not a narrow technical dispute; it is a proxy for a much older question about how much power a society is willing to grant its institutions, public or private, over the private lives of its members. The Apple v. FBI case and the Snowden revelations each showed, in different registers, how quickly abstract policy debates about encryption can become concrete national controversies with lasting legal and industry consequences. As this paper has argued, the most durable insight from three decades of "crypto wars" scholarship is that solutions promising costless access access that would somehow be available to legitimate investigators but closed to everyone else have not withstood technical scrutiny. The more productive path forward lies in targeted, judicially supervised mechanisms, transparent legal authority, harmonized cross-border rules, and an honest acknowledgment that the same civil-liberties principles protecting individuals from government overreach must also constrain the increasingly consequential governance power exercised by private platforms.

REFERENCES

[1] Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Green, M., Landau, S., Neumann, P. G., Rivest, R. L., Schiller, J. I., Schneier, B., Specter, M., & Weitzner, D. J. (2015). Keys under doormats: Mandating insecurity by requiring government access to all data and communications. MIT Computer Science and Artificial Intelligence Laboratory Technical Report, MIT-CSAIL-TR-2015-026.

[2] Borgesius, F. J. Z., & Steenbruggen, W. (2019). The right to communications confidentiality in Europe: Protecting privacy, freedom of expression, and trust. Theoretical Inquiries in Law, 20(1), 291–320. https://doi.org/10.1515/til-2019-0011

[3] Caplan, R., & Gillespie, T. (2020). Tiered governance and demonetization: The shifting terms of labor and compensation in the platform economy. Social Media + Society, 6(2). https://doi.org/10.1177/2056305120935638

[4] Cobbe, J. (2021). Algorithmic censorship by social platforms: Power and resistance. Philosophy & Technology, 34(4), 739–766. https://doi.org/10.1007/s13347-021-00465-1

[5] Cotter, K. (2021). "Shadowbanning is not a thing": Black box gaslighting and the power to independently know and credibly critique algorithms. Information, Communication & Society, 24(15), 2308–2324. https://doi.org/10.1080/1369118X.2020.1775507

[6] Gorwa, R., Binns, R., & Katzenbach, C. (2020). Algorithmic content moderation: Technical and political challenges in the automation of platform governance. Big Data & Society, 7(1). https://doi.org/10.1177/2053951719897945

[7] Helberger, N. (2019). On the democratic role of news recommenders. Digital Journalism, 7(8), 993–1012. https://doi.org/10.1080/21670811.2019.1623700

[8] Kerr, O. S., & Schneier, B. (2018). Encryption workarounds. Georgetown Law Journal, 106(4), 989–1048.

[9] Koops, B.-J. (2023). The right to encryption: Privacy as preventing unlawful access. Computer Law & Security Review, 49, Article 105790. https://doi.org/10.1016/j.clsr.2023.105790

[10] Koops, B.-J., & Kosta, E. (2018). Looking for some light through the lens of "cryptowar" history: Policy options for law enforcement authorities against "going dark." Computer Law & Security Review, 34(4), 890–900. https://doi.org/10.1016/j.clsr.2018.03.007

[11] Liguori, C. (2020). Exploring lawful hacking as a possible answer to the "going dark" debate. Michigan Technology Law Review, 26, 317–352.

[12] McDermott, Y. (2025). Technical backdoors and legal backdoors: Regulating encryption in the United Kingdom. The International Journal of Human Rights. https://doi.org/10.1080/09615768.2024.2444720

[13] Odukale, Bowale. (2024). AI Literacy and Entrepreneurial Innovation: Rethinking Digital Competence for the Knowledge Economy. International Journal of Multidisciplinary Evolutionary Research. 5. 91-108. 10.54660/IJMER.2024.5.1.91-108.

[14] Odukale, Bowale. (2024). The Rise of AI Literacy: Redefining Human Communication Competence in the Algorithmic Age. International Journal of Multidisciplinary Evolutionary Research. 5. 76-90. 10.54660/IJMER.2024.5.1.76-90.

[15] Olatunji, Opeyemi & Odukale, Bowale. (2025). Leveraging Predictive Analytics and AI for SME Growth: A Data-Driven Approach to Business Optimization. World Journal of Advanced Research and Reviews. 25. 1830-1841. 10.30574/wjarr.2025.25.3.0958.

[16] Quintais, J. P., Appelman, N., & Fahy, R. (2022). Using terms and conditions to apply fundamental rights to content moderation. German Law Journal (Forthcoming).

[17] Rudesill, D. S. (2015). Coming to terms with secret law. Harvard National Security Journal, 7, 241–283.

[18] Scott, P. F. (2022). Authorising crime: The Covert Human Intelligence Sources (Criminal Conduct) Act 2021. The Modern Law Review, 85, 1218–1247.

[19] Suzor, N. P. (2018). Digital constitutionalism: Using the rule of law to evaluate the legitimacy of governance by platforms. Social Media + Society, 4(3). https://doi.org/10.1177/2056305118787812

[20] Svantesson, D. J. B. (2021). Law enforcement access to electronic evidence across borders. International Journal of Law and Information Technology, 29(1), 1–22. https://doi.org/10.1093/ijlit/eaab001

[21] van der Sloot, B. (2018). A new approach to the right to privacy, or how the European Court of Human Rights embraced the non-domination principle. Computer Law & Security Review, 34(3), 539–549. https://doi.org/10.1016/j.clsr.2017.12.001