Regulating Social Media as a Policing Tool in Malaysia: Legal Challenges and Operational Realities

Nurfaeroz Idris[1], Su'aida Safei[2]*

[1]Investigation Officer, Sexual, Women, and Child Investigation Division, Criminal Investigation Department, Kuala Lumpur Contingent Police Headquarters, Malaysia

[2] Senior lecturer, Faculty of Law, Universiti Teknologi MARA (UiTM), Shah Alam, Selangor, Malaysia

***Corresponding Author**

DOI: https://doi.org/10.47772/IJRISS.2026.101000200

Received: 16 October 2026; Accepted: 28 October 2026; Published: 31 October 2026

ABSTRACT

The rapid expansion of social media and digital platforms has transformed contemporary law enforcement, enabling police agencies to leverage open-source intelligence (OSINT) and digital analytics for crime detection, investigation, and public engagement. However, utilising social media as a policing tool presents significant legal challenges and operational complexities, particularly regarding statutory boundaries, evidentiary standards, and constitutional safeguards. This qualitative, doctrinal legal research examines the regulatory framework governing digital policing by the Royal Malaysia Police (RMP). Utilising primary statutory provisions—including the Communications and Multimedia Act 1998, Criminal Procedure Code, Computer Crimes Act 1997, and Evidence Act 1950—alongside relevant judicial precedents, this paper examines how Malaysian law balances police operational powers with fundamental liberties guaranteed under the Federal Constitution. Furthermore, the paper conducts a comparative analysis with the United States legal framework, highlighting constitutional standards under the First and Fourth Amendments and statutory thresholds set by the Stored Communications Act. The findings reveal that Malaysia lacks a dedicated, comprehensive legislative framework tailored to digital surveillance and social media intelligence, relying instead on a fragmented matrix of traditional statutes. The paper concludes by recommending targeted legislative reforms, specific operational guidelines for digital intelligence gathering, and continuous digital forensic training to ensure effective law enforcement while safeguarding individual fundamental liberties.

The exponential growth of social media has fundamentally transformed law enforcement strategies, enabling agencies like the Royal Malaysia Police (RMP) to leverage digital platforms for criminal investigations, intelligence gathering, and community engagement. However, the integration of social media into modern policing raises complex legal challenges, particularly concerning individual privacy, freedom of expression, and the admissibility of electronic evidence. This paper evaluates the adequacy of the Malaysian legal framework in regulating social media as a policing tool. Adopting a qualitative and doctrinal approach, the study analyses key Malaysian statutes, including the Communications and Multimedia Act (CMA) 1998, the Evidence Act 1950, and the Penal Code, as well as relevant judicial interpretations. To contextualise these findings, a comparative analysis of the United States legal framework is conducted, focusing on constitutional safeguards and statutory mechanisms such as the Stored Communications Act (SCA). Empirical insights are derived from semi-structured interviews with senior officers from the RMP's Criminal Investigation Department (D5). The findings indicate that while Malaysia's statutory provisions provide sufficient legal authority for cyber investigations, significant operational gaps remain regarding digital evidence preservation, cross-jurisdictional data retrieval, and inter-agency coordination. The paper concludes that introducing robust internal governance, specialised standard operating procedures (SOPs), and continuous digital forensic training is more viable than drafting entirely new legislation.

Keywords: Social media policing, Digital evidence, Communications and Multimedia Act, Royal Malaysia Police, Stored Communications Act, Cybercrime law, Freedom of expression.

INTRODUCTION

The widespread adoption of digital technology and social networking platforms has dramatically altered the landscape of communication and information sharing (Kemp, 2023). In Malaysia, where internet penetration and social media usage are exceptionally high, law enforcement agencies have had to rapidly adapt their operational methodologies. The Royal Malaysia Police (RMP) actively utilises platforms such as Facebook, Instagram, Twitter, and TikTok for public communication, emergency alerts, and intelligence gathering (Azwan et al., 2016). Social media analytics and open-source intelligence (OSINT) allow investigators to identify suspects, trace criminal networks, and corroborate witness statements (Fortin et al., 2023).

However, incorporating social media into daily policing practices poses distinct legal and ethical challenges (Edwards & Urquhart, 2016). Malaysian law enforcement operates under traditional statutes such as the Police Act 1967 (Act 344), which outlines the general duties and powers of police officers in Section 19 but lacks specific provisions for navigating the digital environment. Without precise legislative guidance detailing how online monitoring should be conducted or how long digital intelligence may be retained, law enforcement agencies face the difficult task of balancing operational efficiency with the constitutional rights of individuals (Thukral & Kainya, 2022). Consequently, it is imperative to critically examine how existing laws are operationalised in the context of digital investigations.

OBJECTIVES

This paper has three primary objectives. Firstly, to analyse the existing legal framework in Malaysia regulating the use of social media as a policing tool by the RMP. Secondly, to examine the legal framework in the United States to identify comparative principles relating to digital policing and constitutional safeguards. Thirdly, to suggest practical reforms to improve how social media is governed and utilised by Malaysian law enforcement.

METHODOLOGY

According to Dobinson and Chi, doctrinal or theoretical legal research can be defined in simple terms as research which asks what the law is in a particular area. The researcher seeks to collect and then analyse a body of case law, together with any relevant legislation (so-called primary sources). This may also include secondary sources such as journal articles or other written commentaries on the case law and legislation. The researcher's principal aim is to describe a body of law and how it applies. In doing so, the researcher may also provide an analysis of the law to demonstrate how it has developed in terms of judicial reasoning and legislative enactment. (Dobinson and Chi, 2007). Abdullah later in 2018 summarised that a doctrinal research (also known as pure theoretical research) deals with the law on a particular issue where the legal doctrine is analysed as to its development and applications (Abdullah, 2018).

This paper predominantly employs a doctrinal legal research methodology, utilising an in-depth analysis of Malaysian statutes, judicial decisions, and constitutional frameworks as its primary data source. The primary data used in this paper consist mainly of relevant legislation and case law concerning social media use and enforcement law in Malaysia. The legislation examined includes the Communications and Multimedia Act 1998 (CMA 1998), the Official Secrets Act 1972 (OSA), the Evidence Act 1950, the Criminal Procedure Code (CPC), the Computer Crimes Act 1997, and the Penal Code. Each of these legal sources is examined to determine its relevance to the legal framework that governs the use of social media as a policing tool. Relevant case law also forms part of the primary data. Relevant cases are reviewed to see how the courts have dealt with the interpretation and application of these laws in specific circumstances. The judicial decisions also provide real-world illustrations of legal precedent, which contribute to a better understanding of the legal position regarding the use of social media by law enforcement.

The secondary data for this paper are drawn from scholarly articles, journals, reports, and other academic writings on social media usage, law enforcement, and the legal implications of technology in crime prevention and investigation. These materials are used to consider the subject from a wider perspective. They also

contribute theoretical views, comparative analysis, and critical discussion relevant to the issues examined in this paper.

Both primary and secondary data are used in analysing the issues examined in this paper. The analysis involves careful review and comparison of legal texts, case law and scholarly writings. Particular attention is paid to trends and patterns that emerge from these materials, as well as any inconsistencies or gaps in the laws governing the use of social media as a policing tool. In this way, the paper examines the relevant legal rules and considers how they operate in practice.

Since this paper is qualitative in nature, the collection, organisation and analysis of data are conducted in a systematic manner. The primary data, consisting of legal texts and case law, is first reviewed and organised according to relevant themes and legal provisions. The review then turns to secondary sources, which provide context for the analysis and strengthen understanding of the legal landscape.

This paper employs a qualitative empirical approach integrated with doctrinal legal research. Primary data comprises an in-depth analysis of Malaysian legislation and judicial decisions. To evaluate the practical application of these laws, semi-structured interviews were conducted with two senior officers—Deputy Superintendent of Police (DSP) (referred hereinafter as "Respondent 1") and Assistant Superintendent of Police (ASP) (referred hereinafter as "Respondent 2") —both serving in the Investigation and Legal Division (D5) of the RMP Criminal Investigation Department. The empirical data validates the doctrinal analysis by providing frontline perspectives on the enforcement challenges encountered in social media investigations.

BRIEF ANALYSIS

Malaysia and the United States adopt distinct legal frameworks to regulate social media policing and digital evidence. Malaysia relies on a statutory matrix where the Communications and Multimedia Act 1998, Penal Code, Computer Crimes Act 1997, Sedition Act 1948, and Criminal Procedure Code govern offences, cybercrimes, and search procedures. Additionally, Sections 90A and 90B of the Evidence Act 1950 establish conditions for admitting computer-generated records into court. While Article 10 of the Federal Constitution protects freedom of speech, it remains subject to statutory restrictions for public order and security. Conversely, the U.S. framework is heavily anchored in constitutional safeguards: the First Amendment limits broad speech restrictions on digital platforms, while the Fourth Amendment mandates warrants for accessing digital location data. Procedurally, U.S. law enforcement must satisfy strict statutory thresholds under the Stored Communications Act, Electronic Communications Privacy Act, Computer Fraud and Abuse Act, and Federal Rules of Evidence Rule 901 to access and authenticate electronic evidence.

FINDINGS

The Malaysian Legal Framework

In Malaysia, there is no single comprehensive statute governing social media policing; instead, investigations rely on a matrix of laws depending on the nature of the offence. The Communications and Multimedia Act (CMA) 1998 (Act 588) is the primary regulatory instrument. Section 211 prohibits the provision of offensive, indecent, or menacing content, while Section 233 criminalises the improper use of network facilities (Islam et al., 2020). The application of Section 233 in cases of online incitement was recently affirmed in Public Prosecutor v. John Mule anak Alai (2026).

For traditional crimes extending into the digital sphere, investigators rely on the Penal Code (Act 574)—specifically Sections 499 and 500 for defamation, and Section 505 for statements conducing to public mischief. The Computer Crimes Act 1997 (Act 563) governs cyber-intrusions, with Sections 3 to 6 criminalising unauthorised access and data modification. Where public order and national security are threatened by online posts, the Sedition Act 1948 (Act 15) and the Official Secrets Act 1972 (OSA) become relevant. The Federal Court has consistently held that freedom of expression is subject to statutory restrictions to preserve public

security, principles established in cases such as Public Prosecutor v. Azmi Sharom [2015] 6 MLJ 751 and Public Prosecutor v. Lim Kit Siang [1979] 2 MLJ 37.

Crucially, the Criminal Procedure Code (CPC) (Act 593) provides the procedural authority for search and seizure (Sections 51–62), while the Evidence Act 1950 (Act 56) governs the admissibility of digital records. Sections 90A and 90B establish the parameters for admitting computer-generated documents, as interpreted in Public Prosecutor v. Rutinin bin Suhaimin [2010] 4 MLJ 393 and Hanafi bin Mat Hassan v. Public Prosecutor [2006] 4 MLJ 134, where the courts affirmed that digital evidence is admissible provided statutory authentication requirements are meticulously satisfied.

The United States Comparative Framework and Summary Table

In contrast to Malaysia's statutory reliance, the United States regulatory model is heavily anchored in constitutional protections (Chemerinsky, 2023). The First Amendment safeguards freedom of speech, with the Supreme Court explicitly recognising social media as the "modern public square" in Packingham v. North Carolina, 582 U.S. 98 (2017), thereby preventing overly broad governmental restrictions on platform access. Simultaneously, the Fourth Amendment guards against unreasonable searches. In Carpenter v. United States, 585 U.S. 296 (2018), the Supreme Court ruled that law enforcement generally requires a warrant to access digital historical location records, establishing that digital data held by third parties retains strong privacy protections.

Statutorily, police access to digital information is strictly regulated by the Electronic Communications Privacy Act (ECPA) 1986 and the Stored Communications Act (SCA) 1986 (Kerr, 2004). Section 2703 of the SCA (18 U.S.C. § 2703) mandates precise legal thresholds—requiring a warrant, subpoena, or specific court order—depending on the type of electronic data being sought from service providers.

To clearly illustrate the distinct approaches taken by both jurisdictions, Table 1 summarises the core comparative elements of the legal frameworks governing digital evidence and online communications in Malaysia and the United States.

Table 1: Comparative Analysis of Legal Frameworks (Malaysia vs United States)

Legal Area / Scope	Malaysia (Statutory & Constitutional)	United States (Statutory & Constitutional)
Constitutional Safeguards	**Federal Constitution**: Article 5 protects personal liberty, while Article 10 guarantees freedom of speech, subject to parliamentary restrictions for public order and security.	**US Constitution**: The First Amendment protects freedom of speech, while the Fourth Amendment protects against unreasonable searches and seizures of digital data.
Electronic Communications & Social Media Misuse	**Communications and Multimedia Act 1998 (CMA),** Section 233: Regulates the improper use of network facilities or services, including the misuse of online platforms.	**Stored Communications Act (SCA),** 18 U.S.C. §§ 2701–2712: Governs law enforcement access to and disclosure of electronic communications, mandating a warrant or court order for user data.
Admissibility of Digital Evidence	**Evidence Act 1950 Section 90A:** Allows electronic records, including social media content, to be admitted as evidence in court upon fulfilling authentication conditions.	**Federal Rules of Evidence (FRE) Rule 901:** Requires proof that electronic evidence is genuine before it can be authenticated and admitted in court.
Cybercrime & Unauthorised Access	**Computer Crimes Act 1997:** Criminalises unauthorised access, modification, and misuse of computer systems.	**Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030:** Criminalises unauthorised access, fraud, and cybercrime activities involving computers and online platforms.

Public Order & Investigations	**Penal Code Section 505(b):** Criminalises statements conducive to public mischief, including those disseminated via social media.	**Fourth Amendment to the U.S. Constitution:** Protects against unreasonable searches and seizures, generally requiring warrants to access private communications and digital data.
Procedural Search & Seizure Powers	**Criminal Procedure Code (CPC) Sections 15–50:** Provides general search, seizure, and arrest powers to investigate crimes.	**Federal Rules of Criminal Procedure (Rule 41):** Governs the issuance of warrants for search and seizure, including the procedures for tracking and extracting digital data.
Information Governance	**Official Secrets Act (OSA) 1972:** Protects classified information and restricts disclosure.	**Electronic Communications Privacy Act (ECPA) 1986 & Freedom of Information Act (FOIA) 1966:** Balances the regulation of government access to stored data with public access to certain records.

FINDINGS / RESULTS

The qualitative interviews revealed that social media is an indispensable tool for intelligence-led policing in Malaysia. Respondent 2 confirmed that platforms like Facebook, Threads, and TikTok are routinely monitored to combat online gambling syndicates, unearth illegal call centres, and investigate defamation and child exploitation.

Despite the lack of a singular cyber-policing statute, Respondent 1 stated that the existing framework (CMA, CPC, Evidence Act) provides sufficient legal authority for digital investigations. The primary obstacles are not legislative gaps, but rather enforcement and operational complexities. First, the rapid dissemination of fake news (e.g., on TikTok and YouTube) often outpaces the investigative process, manipulating public order before official verification can occur. Second, there is a fundamental misalignment between the community guidelines of international social media conglomerates and Malaysian statutory law, which complicates and delays data retrieval requests.

Furthermore, the respondents highlighted a critical need for enhanced internal governance. Jurisdictional overlaps between the RMP and the Malaysian Communications and Multimedia Commission (MCMC) sometimes create operational redundancies. Moreover, the lack of specialised, continuously updated RMP standard operating procedures (SOPs) regarding operational security means some personnel lack awareness of the legal boundaries of digital monitoring and the preservation protocols necessary to satisfy the authentication standards established in Public Prosecutor v. Khoo Hi Chiang [2003] 6 MLJ 225.

CONCLUSION / IMPLICATIONS

The integration of social media platforms into the daily operations of the Royal Malaysia Police (RMP) represents an essential adaptation to the realities of modern cyber-enabled crime and digital communication. Open-source intelligence and digital analytics have undoubtedly enhanced criminal investigations, suspect identification, and public safety initiatives. However, as demonstrated in this paper, Malaysia's existing statutory framework governing social media policing remains fragmented. Relying on a patchwork of traditional and cyber-related legislation—such as the Police Act 1967, Criminal Procedure Code, Communications and Multimedia Act 1998, Computer Crimes Act 1997, and Evidence Act 1950—creates legal ambiguities regarding the exact scope of digital monitoring, data retention, and procedural search powers.

While Article 10 of the Federal Constitution guarantees freedom of expression, it remains subject to broad parliamentary restrictions in the interest of public order and national security. In contrast, the comparative analysis of the United States framework highlights how explicit constitutional protections under the First and Fourth Amendments—coupled with structured statutory thresholds like the Stored Communications Act—provide clearer judicial boundaries and privacy safeguards when law enforcement seeks access to electronic

communications. For Malaysia to maintain public trust while ensuring operational efficiency, its regulatory regime must evolve beyond reactive statutory applications. Striking a proportional balance between robust policing capabilities and individual constitutional rights requires dedicated legislative frameworks and clear, standardised guidelines for digital intelligence gathering.

The findings indicate that the RMP possesses adequate statutory power to execute social media policing under current laws. However, applying general statutes crafted before the advent of modern social media to complex digital investigations generates significant enforcement friction. The comparative analysis of the United States framework demonstrates that while Malaysia does not require an identical constitutional structure, establishing clear procedural thresholds for accessing and retaining digital data—akin to the mechanisms in the US Stored Communications Act—would foster greater accountability and public trust. Ultimately, the implication is that legislative overhaul is secondary; the immediate priority is strengthening the RMP's institutional governance, inter-agency collaboration, and technical proficiency to navigate the realities of digital law enforcement.

RECOMMENDATIONS

Based on the legal and comparative findings of this paper, the following practical legal and policy reforms are recommended to enhance the regulation of social media as a policing tool in Malaysia:

1. Enact Specific Legislation or Amendments for Digital Surveillance and open-source intelligence OSINT:

Parliament should enact dedicated provisions within the Police Act 1967 or Criminal Procedure Code (CPC) that explicitly define and regulate digital monitoring, open-source intelligence (OSINT) collection, and digital data retention. Clear statutory thresholds should be established specifying when online monitoring is permissible, ensuring actions are necessary, proportionate, and subject to procedural limits.

2. Formulate Standard Operating Procedures (SOPs) for Digital Intelligence:

The Royal Malaysia Police (RMP) and the Ministry of Home Affairs should develop comprehensive Standard Operating Procedures (SOPs) governing social media intelligence collection. These SOPs must delineate the line between public domain monitoring and invasive digital surveillance, establishing strict guidelines for data storage, chain of custody, and privacy preservation during investigations.

3. Strengthen Judicial Oversight and Search Warrant Requirements:

Drawing insights from the U.S. Fourth Amendment jurisprudence and the Stored Communications Act, Malaysia should introduce explicit statutory requirements mandating police officers to obtain search warrants or judicial orders prior to accessing private digital communications, restricted social media profiles, or metadata from service providers.

4. Standardise Digital-Specific Standard Operating Procedures (SOPs) :

To streamline court proceedings and ensure consistent application of Sections 90A and 90B of the Evidence Act 1950, formal technical guidelines should be established for law enforcement officers. The RMP should implement and periodically review strict SOPs detailing the precise legal parameters for monitoring, extracting, and preserving digital evidence from social media. Standardised digital-specific SOPs will ensure that social media screenshots, metadata, and extracted electronic files meet strict legal authentication standards in criminal prosecutions.

5. Provide continuous technical training for the investigating officers:

Investigating officers require mandatory, ongoing professional development in open-source intelligence (OSINT), digital forensics, and international data request protocols to handle complex cybercrimes effectively (Trottier, 2015). Therefore, their superiors should provide them with continuous technical training in the above-mentioned areas.

1. Develop Digital-Specific SOPs: The RMP should implement and periodically review strict Standard Operating Procedures detailing the precise legal parameters for monitoring, extracting, and preserving digital evidence from social media, ensuring compliance with Section 90A of the Evidence Act 1950.

2. Continuous Technical Training: Investigating officers require mandatory, ongoing professional development in open-source intelligence (OSINT), digital forensics, and international data request protocols to handle complex cybercrimes effectively (Trottier, 2015).

3. Enhance Multi-Agency Collaboration: Formalise clearer jurisdictional boundaries and expedited data-sharing channels between the RMP Criminal Investigation Department, the MCMC, and international technology platform providers to accelerate lawful intelligence retrieval.

ACKNOWLEDGMENT

Both authors express gratitude to Allah Almighty and extend deep appreciation to the Faculty of Law, Universiti Teknologi MARA (UiTM), Shah Alam, Selangor, Malaysia, for the moral support that has helped in the completion of this paper.

and the officers of the Investigation and Legal Division (D5), Criminal Investigation Department at Bukit Aman, for their vital cooperation and professional insights.

REFERENCES

1. Abdullah, N.C. (2018). Legal Research Methodology. Thomson Reuters Asia Sdn Bhd
2. Azwan, A., Safar, H. A., & Rahman, N. A. (2016). The roles of social media in crime issues in Malaysia: A study at higher learning institutions in Negeri Sembilan, Melaka, and Johor. Journal of Global Business and Social Entrepreneurship (GBSE), 1(2), 99-106.
3. Brayne, S. (2018). Big data surveillance: The case of policing. American Sociological Review, 82(5), 977-1008.
4. Carpenter v. United States, 585 U.S. 296 (2018).
5. Chemerinsky, E. (2023). Constitutional law: Principles and policies (7th ed.). Aspen Publishing.
6. Communications and Multimedia Act 1998 (Act 588) (Malaysia).
7. Computer Crimes Act 1997 (Act 563) (Malaysia).
8. Dobinson, I. and Chi, W.H.(2007). Qualitative Legal Research. In McConville,M. and Chui. W.H. Research Methods for Law(pp. 16-45). Edinburgh University Press
9. Edwards, L., & Urquhart, L. (2016). Privacy in public spaces: What expectations of privacy do we have in social media intelligence? International Journal of Law and Information Technology, 24(3), 279-310.
10. Evidence Act 1950 (Act 56) (Malaysia).
11. Fortin, F., Boivin, R., & Faubert, C. (2023). Social media use in law enforcement investigations: Opportunities and challenges. Police Practice and Research, 24(2), 145-162.
12. Hanafi bin Mat Hassan v. Public Prosecutor [2006] 4 MLJ 134 (Malaysia).
13. Islam, M. Z., Zulhuda, S., Afandi, N. H. M. B., & Shafy, M. A. (2020). Ensuring safe cyberspace for children: An analysis of the legal implications of social media usage in Malaysia and Singapore. IIUM Law Journal, 28(S1), 395-413.
14. Kemp, S. (2023). Digital 2023: Global overview report. DataReportal. Retrieved from https://datareportal.com/reports/digital-2023-global-overview-report on 22 October 2026
15. Kerr, O. S. (2004). A user's guide to the Stored Communications Act, and a legislator's guide to amending it. The George Washington Law Review, 72(6), 1208-1243.
16. Packingham v. North Carolina, 582 U.S. 98 (2017).
17. Penal Code (Act 574) (Malaysia).
18. Public Prosecutor v. Azmi Sharom [2015] 6 MLJ 751 (Malaysia).
19. Public Prosecutor v. John Mule anak Alai (2026) Sessions Court Miri (Malaysia).
20. Public Prosecutor v. Khoo Hi Chiang [2003] 6 MLJ 225 (Malaysia).
21. Public Prosecutor v. Lim Kit Siang [1979] 2 MLJ 37 (Malaysia).

22. Public Prosecutor v. Rutinin bin Suhaimin [2010] 4 MLJ 393 (Malaysia).
23. Solove, D. J., & Schwartz, P. M. (2021). Information privacy law (7th ed.). Wolters Kluwer.
24. Thukral, P., & Kainya, V. (2022). How social media influence crimes. Indian Journal of Law and Legal Research, 4(2). Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4107673 on 22 October 2026
25. Trottier, D. (2015). Open source intelligence, social media and law enforcement: Visions, constraints and critiques. European Journal of Cultural Studies, 18(4-5), 530-547.