AMERICAN JOURNAL OF EDUCATION AND LEARNING
ISSN: 2996-5128 (online) | ResearchBib (IF) = 10.91 IMPACT FACTOR
Volume-3| Issue-7| 2025 Published: |30-07-2025|

CYBERCRIME AND HUMAN RIGHTS: BALANSING SECURITY AND PRIVACY IN INTERNATIONAL COOPERATION

https://doi.org/10.5281/zenodo.16959156

Gulimova Dilshoda Alloyor Qizi
Master's Student, University of World Economy and Diplomacy, Faculty of International Law

Abstract

This article examines the tension between law enforcement needs and human rights protections in cross-border cooperation to combat cybercrime. It analyses international legal instruments, key institutional practices, and recent developments in surveillance and digital evidence handling. Based on international reports and case-law, the paper proposes policy recommendations to strengthen cooperation while safeguarding privacy and fundamental freedoms.

Keywords

cybercrime; human rights; international cooperation; digital evidence; surveillance

The rapid digitalisation of economies and societies has expanded opportunities for criminal activity, while simultaneously presenting novel challenges for law enforcement. Transnational cybercrime—ransomware, fraud, intrusion and data theft—requires coordinated international responses. However, cooperation between states and with private sector actors raises pressing human rights concerns, notably the right to privacy, freedom of expression, and procedural safeguards. This article explores how international cooperation mechanisms can be designed and practised to achieve an appropriate balance between security and fundamental rights.

Recent literature emphasises three interlocking trends: (1) a global increase in the scale and sophistication of cyber-enabled crime; (2) intensified use of digital surveillance and investigative tools by states; and (3) a growing debate on legal and procedural safeguards for digital evidence and cross-border data requests. Major law enforcement assessments and UN agencies corroborate the rise in cyber-enabled frauds and the expanding role of organised crime groups, while normative bodies stress human-rights risks inherent in mass surveillance and intrusive cyber-tools.

AMERICAN JOURNAL OF EDUCATION AND LEARNING
ISSN: 2996-5128 (online) | ResearchBib (IF) = 10.91 IMPACT FACTOR
Volume-3| Issue-7| 2025 Published: |30-07-2025|

The Budapest Convention on Cybercrime (2001) remains the most comprehensive treaty framework supporting transnational cooperation in cybercrime investigations, including provisions on procedural powers, mutual legal assistance and expedited preservation of data. Simultaneously, the United Nations has been advancing multilateral instruments and operational networks through UNODC to enhance cooperation with a broader constituency of states.

Human-rights concerns arise at multiple stages: overbroad surveillance laws; extraterritorial access to data; inadequate judicial oversight of mutual legal assistance requests; and challenges in ensuring chain of custody, transparency and remedies for affected individuals. The OHCHR has repeatedly warned about spyware and invasive surveillance technologies that can gravely interfere with privacy and other rights.

International Practices and Case Studies

This expanded section provides detailed case studies demonstrating how international cooperation to combat cybercrime has produced both operational successes and significant human-rights tensions. The case studies are grouped into:

(A) judicial/constitutional rulings shaping surveillance limits;

(B) cross-border operational cooperation and emergency takedowns; and

(C) controversies around spyware and private-sector involvement.

(D) A. Judicial and Constitutional Limits on Surveillance

1. European Court of Human Rights — Zakharov v. Russia (2015). In Roman Zakharov v. Russia the ECtHR held that the Russian legal framework for interception of mobile telephone communications lacked adequate safeguards against arbitrary state interference with private life. The Court stressed that even the potential for secret and indiscriminate interception engages Article 8 rights and requires effective safeguards. Zakharov influenced subsequent strictures on bulk surveillance regimes across Europe and highlighted the need for procedural guarantees and independent oversight.[1]

2. European Court of Human Rights — Big Brother Watch & Others v. United Kingdom (Grand Chamber, 2021).

The Grand Chamber concluded that aspects of the UK's bulk interception regime did not provide sufficient 'end-to-end' safeguards to protect against arbitrariness and abuse. The judgment emphasised the importance of clarity, necessity and proportionality in surveillance laws and required improvements in transparency and remedy mechanisms for those affected by mass data collection.[2]

3. *United States — Carpenter v. United States (2018).*

In a landmark decision the US Supreme Court recognised that acquisition of

AMERICAN JOURNAL OF EDUCATION AND LEARNING
ISSN: 2996-5128 (online) | ResearchBib (IF) = 10.91 IMPACT FACTOR
Volume-3| Issue-7| 2025 Published: |30-07-2025|

historical cell-site location information (CSLI) constituted a search under the Fourth Amendment and generally required a warrant supported by probable cause. Carpenter marked a departure from a broad third-party doctrine and has been cited in debates over judicial authorization for access to third-party-held digital records.[3]

These judicial developments underline a growing judicial sensitivity to the privacy implications of modern investigative techniques. They also create practical tension: law enforcement agencies argue that judicial barriers slow urgent investigations, while privacy advocates contend that robust warrants and oversight are necessary to prevent abuse.

B. Cross-border Operational Cooperation: Successes and Oversights

1. INTERPOL and Europol coordinated operations.

Large-scale takedown operations, such as INTERPOL's Operation Synergia II (April–August 2024) and numerous Europol-coordinated actions, have demonstrated the capacity of international cooperation to disrupt criminal infrastructure — from botnets and phishing networks to ransomware affiliates. Operation Synergia II removed tens of thousands of malicious endpoints and involved private-sector cooperation for rapid mitigation.[4][5]

2. *Mutual Legal Assistance and Preservation Orders.*

Mutual Legal Assistance (MLA) remains a workhorse for cross-border investigations, but case-level experience shows that MLA is often slow and hampered by incompatible legal standards, divergent privacy protections, and resource constraints. To address urgent needs, many countries rely on expedited preservation orders and direct cooperation with service providers, which can, however, bypass judicial scrutiny and create accountability gaps.

C. Spyware, Private-Sector Tools and Accountability Gaps

1. Commercial spyware scandals (Pegasus and peers).

The last decade revealed the proliferation of commercial spyware with extrajudicial uses against journalists, dissidents and civil society. OHCHR and UN mandates raised concerns about the use of tools that can turn smartphones into '24-hour surveillance devices', and stressed the absence of meaningful oversight in many states.[6]

2. Private sector role: hosting, data requests, and disclosure tensions.

Technology companies are frequently on the front line: they receive cross-border data requests, may be asked to assist in rapid takedowns, and sometimes face conflicting legal obligations across jurisdictions (e.g., data localisation rules,

secrecy orders). The Schrems II ruling of the Court of Justice of the European Union (CJEU) (2020) - which invalidated the EU-US Privacy Shield - underscored how divergent privacy protections and transnational data transfer rules affect operational cooperation and the flow of evidence across borders.[7]

Lessons from the Case Studies

1. Judicial oversight matters — courts in multiple jurisdictions now require more robust safeguards for bulk or intrusive surveillance, which has spill-over consequences for cross-border investigations.
2. Operational effectiveness can be preserved without abandoning rights: targeted preservation, narrow requests, and improved MLA channels have all proven effective in specific operations.
3. Accountability gaps persist where private spyware and opaque authorisations are involved: states and companies must be subject to independent oversight and redress mechanisms to prevent abuse.

The case studies illustrate the central theme of this article: international cooperation is indispensable to combat cybercrime, but it must be anchored in human-rights protective frameworks that ensure necessity, proportionality and effective remedy.

Several mechanisms can mitigate human-rights risks while preserving investigative efficacy: (a) strong judicial oversight and clear standards for proportionality; (b) transparency measures and reporting obligations; (c) narrow and specific preservation orders; (d) data minimisation and targeted requests; (e) mechanisms for cross-border oversight and mutual accountability; and (f) enhanced public-private collaboration with binding accountability clauses.

7. Recommendations

Policymakers should harmonise legal standards to ensure minimum safeguards for privacy and due process in MLA and mutual legal assistance, invest in capacity building for judicial and law-enforcement actors on digital rights, and strengthen multilateral oversight—including independent audit mechanisms for cross-border data access requests. Furthermore, operational cooperation should embed human-rights impact assessments prior to large-scale surveillance or takedown operations.

Effective international cooperation against cybercrime is both necessary and feasible, but it must be pursued within a framework that respects human rights. Achieving the right balance requires legal safeguards, institutional accountability, and continued multi-stakeholder dialogue. Only then can states jointly address

cyber threats without undermining the fundamental liberties they are meant to protect.

FOOTNOTES

[1] Roman Zakharov v. Russia, ECtHR, Application no. 47143/06, Judgment of 4 December 2015. HUDOC. □cite□turn0search4□

[2] Big Brother Watch and Others v. the United Kingdom, Grand Chamber, HUDOC. □cite□turn0search3□

[3] Carpenter v. United States, 585 U.S. ___ (2018). Supreme Court of the United States. □cite□turn0search5□

[4] INTERPOL, Operation Synergia II press release (2024) and INTERPOL Annual Report 2023. □cite□turn0search15□turn0search7□

[5] Europol, Internet Organised Crime Threat Assessment (IOCTA) 2024. □cite□turn0search9□

[6] OHCHR, 'Spyware and surveillance: Threats to privacy and human rights' (2022) and related UN statements. □cite□turn0search2□turn0search10□

[7] Court of Justice of the European Union, Schrems II (Case C-311/18), Judgment of 16 July 2020. □cite□turn0search6□

[8] Daniel J. Solove, 'A Taxonomy of Privacy', University of Pennsylvania Law Review (2006). □cite□turn1search0□

[9] Orin Kerr, commentary on Carpenter and Fourth Amendment jurisprudence (SSRN). □cite□turn1search1□

[10] Bruce Schneier, essays and commentary on surveillance and privacy (schneier.com). □cite□turn1search2□turn1search5□

REFERENCES

1. Council of Europe. (2001). Convention on Cybercrime (Budapest, 23 November 2001). https://rm.coe.int/1680081561

2. Europol. (2024). Internet Organised Crime Threat Assessment (IOCTA) 2024. https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024

3. INTERPOL. (2023). INTERPOL Annual Report 2023. https://www.interpol.int/

4. OHCHR. (2022). Spyware and surveillance: Threats to privacy and human rights. https://www.ohchr.org/

5. Supreme Court of the United States. (2018). Carpenter v. United States, 585 U.S. ___ (2018). https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf

6. Court of Justice of the European Union. (2020). C-311/18 Schrems II. https://curia.europa.eu/

7. Solove, D. J. (2006). A Taxonomy of Privacy. University of Pennsylvania Law Review.

8. Kerr, O. S. (2018). Implementing Carpenter. SSRN.