p-ISSN:2708-2091
e-ISSN:2708-3586

www.gsrjournal.com
GSR
Global Sociological Review

GSR

GLOBAL SOCIOLOGICAL REVIEW

HEC-RECOGNIZED CATEGORY-Y

VOL. X ISSUE III, SUMMER (SEPTEMBER-2025)

Double-blind Peer-review Research Journal
www.gsrjournal.com

DOI (Journal): 10.31703/gsr
DOI (Volume): 10.31703/gsr.2025(X)
DOI (Issue): 10.31703/gsr.2025(X-III)

HumanityPublications
sharing research

Humanity Publications (HumaPub)
www.humapub.com
Doi: https://dx.doi.org/10.31703

Article title

Cyber Surveillance and the Freedom of Speech: Evaluating Pakistan's PECA 2016 and the UK's Investigatory Powers Act 2016 under Human Rights Standards

Abstract

In an unprecedented manner, this research critically assesses cyber-surveillance and freedom of expression, contrasting Pakistan's Prevention of Electronic Crimes Act (PECA) 2016 with the United Kingdom's Investigatory Powers Act (IPA) 2016. In both jurisdictions, the extent to which national security priorities compete with the human rights of Free Speech and expression is explored through the relevant legal frameworks. The inquiry touches upon whether these surveillance practices meet international human-rights standards while zooming in on legal vagueness, surveillance issues, and lack of accountability. Therefore, it concludes that strong safeguards and a transparent regulatory mechanism must be urgently put in place to counter the abuse of such powers while fostering fundamental freedoms in the digital age.

Keywords: Cyber Surveillance, Freedom of Speech, PECA 2016, Investigatory Powers Act 2016, Human Rights Standards, Data Retention, Judicial Oversight

Authors:

Naveed Ejaz: (Corresponding Author)
PhD Scholar, Department of Law, Islamiya University Bahawalpur, Punjab, Pakistan.
(Email: nidoojaz@gmail.com)

Pages: 115-126
DOI: 10.31703/gsr.2025(X-III).12
DOI link: https://dx.doi.org/10.31703/gsr.2025(X-III).12
Article link: http://www.gsrjournal.com/article/cyber-surveillance-and-the-freedom-of-speech-evaluating-pakistans-peca-2016-and-the-uks-investigatory-powers-act-2016-under-human-rights-standards
Full-text Link: https://gsrjournal.com/article/cyber-surveillance-and-the-freedom-of-speech-evaluating-pakistans-peca-2016-and-the-uks-investigatory-powers-act-2016-under-human-rights-standards
Pdf link: https://www.gsrjournal.com/jadmin/Auther/31rvIolA2.pdf

Global Sociological Review
p-ISSN: 2708-2091 **e-ISSN:** 2708-3586
DOI(journal): 10.31703/gsr
Volume: X (2025)
DOI (volume): 10.31703/gsr.2025(X)
Issue: III Summer (September-2025)
DOI(Issue): 10.31703/gsr.2024(X-III)

Home Page
www.gsrjournal.com

Volume: (2025)
https://www.gsrjournal.com/Current-issues

Issue: III-Summer (June -2025)
https://www.gsrjournal.com/issue/10/3/2025

Scope
https://www.gsrjournal.com/about-us/scope

Submission
https://humaglobe.com/index.php/gsr/submissions

Visit Us

Humanity Publications (HumaPub)
www.humapub.com
Doi: https://dx.doi.org/10.31703

Citing this Article

12	Cyber Surveillance and the Freedom of Speech: Evaluating Pakistan's PECA 2016 and the UK's Investigatory Powers Act 2016 under Human Rights Standards		
Authors	Naveed Ejaz	DOI	10.31703/gsr.2025(X-III).12
		Pages	115-126
		Year	2025
		Volume	X
		Issue	III

Referencing & Citing Styles

APA	Ejaz, N. (2025). Cyber Surveillance and the Freedom of Speech: Evaluating Pakistan's PECA 2016 and the UK's Investigatory Powers Act 2016 under Human Rights Standards. *Global Sociological Review*, *X*(III), 115-126. https://doi.org/10.31703/gsr.2025(X-III).12
CHICAGO	Ejaz, Naveed. 2025. "Cyber Surveillance and the Freedom of Speech: Evaluating Pakistan's PECA 2016 and the UK's Investigatory Powers Act 2016 under Human Rights Standards." *Global Sociological Review* X (III):115-126. doi: 10.31703/gsr.2025(X-III).12.
HARVARD	EJAZ, N. 2025. Cyber Surveillance and the Freedom of Speech: Evaluating Pakistan's PECA 2016 and the UK's Investigatory Powers Act 2016 under Human Rights Standards. *Global Sociological Review,* X**,** 115-126.
MHRA	Ejaz, Naveed. 2025. 'Cyber Surveillance and the Freedom of Speech: Evaluating Pakistan's PECA 2016 and the UK's Investigatory Powers Act 2016 under Human Rights Standards', *Global Sociological Review*, X: 115-26.
MLA	Ejaz, Naveed. "Cyber Surveillance and the Freedom of Speech: Evaluating Pakistan's Peca 2016 and the Uk's Investigatory Powers Act 2016 under Human Rights Standards." *Global Sociological Review* X.III (2025): 115-26. Print.
OXFORD	Ejaz, Naveed (2025), 'Cyber Surveillance and the Freedom of Speech: Evaluating Pakistan's PECA 2016 and the UK's Investigatory Powers Act 2016 under Human Rights Standards', *Global Sociological Review,* X (III), 115-26.
TURABIAN	Ejaz, Naveed. "Cyber Surveillance and the Freedom of Speech: Evaluating Pakistan's Peca 2016 and the Uk's Investigatory Powers Act 2016 under Human Rights Standards." *Global Sociological Review* X, no. III (2025): 115-26. https://dx.doi.org/10.31703/gsr.2025(X-III).12.

e-ISSN: 2708-2091 Volume: X (2025) Issue: III-Summer (September -2025) p-ISSN: 2708-3586

Global Sociological Review
www.gsrjournal.com
DOI: http://dx.doi.org/10.31703/gsr

Pages: 115-126 URL: https://doi.org/10.31703/gsr.2025(X-III).12 Doi: 10.31703/gsr.2025(X-III).12

Title

Cyber Surveillance and the Freedom of Speech: Evaluating Pakistan's PECA 2016 and the UK's Investigatory Powers Act 2016 under Human Rights Standards

Authors:

Naveed Ejaz
(Corresponding Author)
PhD Scholar, Department of Law, Islamiya University Bahawalpur, Punjab, Pakistan.
(Email: nidoojaz@gmail.com)

Contents

Abstract

In an unprecedented manner, this research critically assesses cyber-surveillance and freedom of expression, contrasting Pakistan's Prevention of Electronic Crimes Act (PECA) 2016 with the United Kingdom's Investigatory Powers Act (IPA) 2016. In both jurisdictions, the extent to which national security priorities compete with the human rights of Free Speech and expression is explored through the relevant legal frameworks. The inquiry touches upon whether these surveillance practices meet international human-rights standards while zooming in on legal vagueness, surveillance issues, and lack of accountability. Therefore, it concludes that strong safeguards and a transparent regulatory mechanism must be urgently put in place to counter the abuse of such powers while fostering fundamental freedoms in the digital age.

Keywords: Cyber Surveillance, Freedom of Speech, PECA 2016, Investigatory Powers Act 2016, Human Rights Standards, Data Retention, Judicial Oversight

Introduction

In the digital age, cyber-surveillance is the most significant and indispensable mechanism of power for the state. This is a medium that alters dramatically the manner in which governments investigate crime, protect national security, and administer information risk. These methods, however, lead to the most paradoxical, and, in fact, now completely conjured capacities for the collection and cataloging of minutiae about people's lives-whether by the means of network monitoring, metadata retention, device searches, and compelled decryption. The present study takes a comparative inquiry into the Prevention

of Electronic Crimes Act 2016 (Government of Pakistan, 2016), in Pakistan, against the UK Investigatory Powers Act 2016 (IPA 2016), against the scale of international human rights standards. The question, simple but heavily loaded in terms of implications, is: to what extent can one accommodate the two statutes to reconcile effective policing through cyber-enable means with Freedom of Speech and such freedoms associated with it, such as expression, association, and due process? (Aleem et al., 2023)

The inquiry is within a standard of legality, legitimacy, necessity, and proportionality, which are the four tests derived from international human rights jurisprudence. Article 17 of the International Covenant on Civil and Political Rights (ICCPR) prohibits arbitrary or unlawful interference with privacy; similar protections are contained in Article 8 of the European Convention on Human Rights (ECHR), which continues to inform UK practice. All those instruments converge into a common architecture: secret surveillance must be "in accordance with law", pursue a legitimate aim (e.g., national security or serious crime), be necessary in a democratic society (i.e., strictly required), and be proportionate, accompanied by robust ex-ante authorization and ex-post oversight. (Milanovic, 2018)

Pakistan's constitutional order proudly holds its own privacy guarantees within itself. Article 14 guarantees dignity of man and more specifically, the privacy of the home. Courts have thus extrapolated wider privacy interest from this principle. Thus, present-day surveillance law in Pakistan rests on two pillars: on the one hand, the Fair Trial Act, 2013 contains a warrant framework for interception of communications by designated agencies and on the other, PECA, 2016, defines electronic crimes and investigative powers while also laying out data-related obligations for service providers. Among core PECA surveillance-adjacent provisions include powers for search and seizure of digital systems, preservation and retention of traffic data, and cooperation obligations imposed on intermediaries (Iqbal et al., 2023).

Criticism of the framework in Pakistan matches familiar human rights concerns. First, often, such standards under which any intrusion is allowed tend to be very high level and hence are prone to wide application to real-world technologies. Second, the interface between PECA and general criminal procedure provides for potential gaps regarding scope of warrants-device-wide vs. file-specific-as well as on-device search and chain of custody and integrity of digital evidence. Third, retention mandates and preservation orders raise the possibility of questions surrounding the mass collection versus targeted measures, duration, and security of retained data, and the absence of independent, specialized oversight with technical capacity. Finally, the scant openness exists: limited publication duties exist in regards to the volume and legal basis determining demands from the state, while persons affected are rarely informed later on, allowing them to dispute the surveillance or seek remedies. These features raise questions about whether intrusions are indeed strictly necessary and proportionate in practice (Murphy, 2015).

The IPA 2016 was launched as a completely comprehensive statute to bring all existing surveillance powers into one fully updated, comprehensive statute after decades of ad-hoc lawmaking and ground-breaking judgments from the courts. Its most distinguishing components range from targeted interception and equipment interference, into bulk powers (bulk interception, bulk acquisition of communications data, bulk equipment interference), retention of Internet Connection Records, and prescribed systems of notices compelling technical capabilities or retention from providers. The "double-lock"-political authorization by a Secretary of State followed by approval from a Judicial Commissioner-is meant to satisfy the legality and necessity-proportionality tests while institutional oversight is given by the Investigatory Powers Commissioner's Office (IPCO). (Looney, 2025).

The UK regime has continued to face scrutiny on human rights issues even with these guardrails. The courts have noted that a general or indiscriminate retention and bulk acquisition would call for stringent

conditions, including strong targeting, filtering, and minimization rules, and would need further safeguards in cases where examination communication was entailed for people in the UK or sensitive professions. The standards of independent authorization, security of data, retention periods, and access controls become extremely important; if those standards are weak or unclear, then necessary surveillance will tip into disproportionate surveillance (White, 2024).

A rights-based approach also foregrounds collaterals. The speaking rights are chilled when an individual fears that his/her browsing history, contacts, location, or contents of the device might be opened up to scrutiny not strictly necessary. It may repress civic associations, investigative journalism, and political participation, particularly in places with low legal thresholds or patchily enforced laws. Both the content-blocking powers of the PECA and the retention/acquisition architecture of the IPA would at an indirect level pressure platforms and providers toward over-compliance resulting in private censorship and function creep. Such a regime of human rights compliance will, there-fore, require better warrants and oversight, narrow technology-specific drafting, strong provider-user transparency, duties of security and deletion, and remedies approachable without dependency on secret litigation or special tribunals closed to the public (White, 2024).

Research Questions

1. To what extent do PECA 2016 and IPA 2016 align with international human rights standards on expression?
2. Are the surveillance powers (interception, data retention, bulk powers) necessary and proportionate?
3. How effective are oversight, transparency, and redress mechanisms?

Methodology

Using a doctrinal approach towards a comparative examination of cybersurveillance acts and the Freedom of Speech under the Prevention of Electronic Crimes Act 2016 and the Investigatory Powers Act 2016 of the United Kingdom, the study is based on the scrutiny and critical analysis of primary sources of law. These primary sources include constitutional provisions of privacy protections, surveillance laws, and related judicial precedents on the question of state power. This method further evaluates the incompatibility of the two pieces of legislations with established human rights norms as contained in several international human rights treaties, namely, the International Covenant on Civil and Political Rights (ICCPR) and the European Convention on Human Rights (ECHR) by way of a systematic examination of the two legislations' constitutional text and provisions. It involves employing leading commentaries, legislative debates, and explanations thereof for understanding of legislative intent and thus presents a normative evaluation of the balance struck between national security imperatives and individual privacy.

Theoretical & Normative Framework

Modern cyber security systems must be accessed via the multiple layers of a normative framework that links (1) fundamentality principles of human rights (the legal "why") to (2) principles of legality and necessity to (3) institutional safeguards and remedies. Such a framework allows the comparative evaluation of statutory regimes like the Prevention of Electronic Crimes Act, 2016 (PECA) of Pakistan and its counterpart, the Investigatory Powers Act, 2016 (IPA) in the United Kingdom.

The first dimension: Normative substance of the Freedom of Speech. International human rights law regards privacy, not as a right absolute, but as one that protects individuals against arbitrary or unlawful interference in their private life, correspondence and reputation. Those interfering with the ICCPR and with regional instruments must be guided by the following principles: those interfered with must be foreseen through law, and the aims must respect and protect constitutionally created allocations, introducing the interference of necessity and proportionality at runtime within the socio-political

environment of Europe. Beyond those tripartite tests, UN guidance brings up the digital context, wherein indiscriminate, bulk, and/or secret surveillance coexist with acute risks to freedom of expression, association, and other civil liberties requiring stronger justification and heightened safeguards (White, 2024).

Doctrinally: legality, necessity, proportionality and specificity. "Prescribed by law" means fulfilled by way of statute, but it requires more than that: the law must be accessible, precise, and foreseeable, allowing individuals to conform their behavior according to the law and courts to implement those limits. Necessity and proportionality lie along a spectrum; an interception directed at a named suspect for a limited time may be justified differently than a mass collection or long-term retention of meta-data. The human-rights doctrine also requires measures that infringe upon basic rights to have been authorized in advance, transparently display the underlying legal principles for doing so, and afford remedies to those who are subjected to the surveillance.(Tariq, 2021)

The institutional level: supervision, responsibility and remedies. In order to effectively realize human rights, the relevant institutional architecture will have to be adopted: independent judicial review on warrants; enlistment by Parliament; independent commissioners with investigatory powers; transparent reporting systems; and remedies being accessible shortly for victims. The independent tribunal, ex-post evaluation, and publication of aggregate statistics will then serve as compensatory safeguards to restrain the untrammeled accumulation of power behind a veil of secrecy. The civil society will be allowed to intervene in front of the independent scrutiny- preferably on a periodic basis- which could pose later as indicators of democratic legitimacy and legal maturity. (Wetzling & Vieth, 2021)

The drama behind PECA 2016: The Act embodies an exhaustive electronic crime penal code endowed with powers for interception of data, takedown orders, blocking and imposition of criminal liability for online speech. The very letter of the statute, and its application as well, have engendered serious normative problems. PECA describes vaguely defined offences, along with giving executive actors very broad takedown and blocking powers to then remove content or force intermediaries to hand over user data. Civil society organizations and human rights organizations have documented cases of PECA being used to criminalize dissent in the speech against journalists. It creates a disreputable mostrud to the very notion of foreseeability and proportionality. This raises concerns about clear conceptualization and precisely tailoring according to the requirement set out in the principle of "prescribed by law" and real pitfalls for arbitrary application (White, 2024).

PECA has deficiencies compared to the doctrinal tests in the following manner: 1) Legality/predictability vague definitions of offences and the broad discretionary powers of the executive make the law vaguely foreseeable as far as its application is concerned; 2) Necessity/proportionality — needless to say there are more limited options that would be equally efficacious. Criminal sanctions to curb certain forms of online expression are made ineffective by lax application of takedown orders; 3) Safeguards/remedies The deficiencies of the surveillance oversight machinery that therefore exist under PECA in Pakistan utterly lack pre-authorization by an independent judicial authority, meaningful transparency, and effective redress as called for by international standards.(Rachel, 2018)

Application of the Framework to the Investigatory Powers Act 2016 in the UK: The IPA constructs a comprehensive statutory scheme governing interception, interference with equipment, or obtaining communications data. More importantly, the IPA codified the judicial oversight, imposed statutory codes of practice, and established express provisions for oversight bodies and retention periods. In this context, and with reference to its legislative design, the IPA would meet the requirement "prescribed by law" through statutory provisions that were detailed as well as provisions for institutional oversight.

Ends of the scale of compliance with human rights standards, IPA is the most evolved response of institutions: there is statutory clarity, and warrants have been judicialized, and there are established oversight mechanisms. While Pakistan's PECA has

vague offences and a lot of executive discretion before weak independent oversight, it faces a high threat of arbitrary or disproportionate interference. However, both manage to show a common malaise of contemporary times both which are: an inclination to engrain powers for bulk collection or technical assistance without proper transparency or redress measures; and the turning to grounds of secrecy and national security which restricts public and judicial scrutiny.

Everywhere in the law for mutual surveillance (PECA-style or IPA-style) must: (1) invasions of privacy must be precisely and narrowly defined; (2) interception and interference with equipment must be independently authorized in advance; (3) the necessity and proportionality tests must be stringently applied, with written justification; (4) retention must be restricted, and technical minimums must be imposed; (5) more care should be taken with vulnerable groups (journalists, lawyers, activists); (6) independent oversight bodies should be created to investigate and impose sanctions; and (7) there should be accessible remedies for aggrieved individuals, as well as public transparency reporting. The principles transform abstract human rights principles into practical legal architecture and tend to balance against the democratic deficit that could be introduced by surveillance power. (Cannataci, 2017).

Doctrinal Overview of PECA 2016

Conceived in 2016 in Pakistan and enveloped in the gradual growth of an ever-increasing digital civilization, the Prevention of Electronic Crimes Act (PECA) was supposed to manage the unfolding web of complexities emerging out of cybercrime. By the time the Law came into effect, it was hailed as an all-encompassing framework designed for the criminalization of a whole range of electronic offences: hacking, data breaches, and identity theft on the content side; cyber-harassment and hate speech, and child sexual abuse material. The Act conferred investigatory powers on law enforcement agencies, particularly the Federal Investigative Agency (FIA), while conferring the regulation of online content on the Pakistan Telecommunication Authority (PTA).

That much was obvious: PECA's intended purpose was to take the law as an instrument to counter the increased incidents of cybercrime in Pakistan. Before PECA was introduced, electronic crimes were basically dealt with in the Pakistan Penal Code and some other loose but quite ineffective provisions in this age of digitalization. PECA has brought together these scattered laws and makes the provisions for criminal liability for acts like hacking, cyber-terrorism, improper use of information systems, spamming, spoofing and dissemination of harmful content on the web. So in this sense, it seemed an honest attempt to synchronize Pakistani law with the world's trends on cybercrimes. However, the Act does not focus only on trespass and theft in the digital context; it has gone much beyond and regulates a wide range of online expression criminalizing various forms of speech including from obscenity to defamation to even the vaguely defined category of "false information."(Khan, 2018)

PECA, inter alina, thus empowers the state institutions with powers of investigation and enforcement. They have been empowered to search premises, seize equipment, intercept communications and compel service providers to disclose user data. Doctrinally these provisions embody the coercive powers of the State in cyberspace. However, with innumerable processes not facing serious judicial or independent scrutiny, this raises serious concerns regarding their application in real human rights situation. Under the international law, both the interception or surveillance or access to personal communications must be governed by strict regulation and pre-approval by an independent judicial body based upon the principles of necessity and proportionality (Khan, 2018).

Another area in which the structure of PECA differs doctrinally from human rights norms is in regard to freedom. In essence, it provides open-ended access to user data, permits interception of communications, and mandates service providers to provide the access. Though national security and

crime prevention are legitimate aims, PECA does not incorporate into itself reasonable safeguards against misuse. Such a rights-compliant regime would explicitly delimit the subject of surveillance, fix time-bound warrants, maintain independent oversight, and delete data once it has lost its evidentiary value. Conversely, PECA generally allows for broad margins of discretion for investigating agencies, often with very limited accountability mechanisms in place (Karabacak et al., 2016).

PECA would further affect the guarantees of due process and fair trial from a doctrinal perspective. In this respect, PECA would be accused of being a criminal statute that creates specific offences that carry grave penalties, including imprisonment. The fundamental rights to presumption of innocence, to timely access to counsel, and to the fair trial protections available under domestic constitutional law and international human rights law would then be activated in this respect for the accused. Moreover, considering that much of the evidence relied upon under PECA shall be electronic, then there exist firm rules to set handling, preservation, and admissibility. Weaknesses in chain-of-custody rules or forensic standards risk wrongful convictions and miscarriages of justice. Further, PECA empowers the PTA and FIA to directly issue blocking orders or takedown requests without necessarily involving the judiciary in a timely manner, resulting in affected persons or platforms having less redress avenues (Karabacak et al., 2016).

PECA has its failings but is not completely incompatible with human rights standards. It is concerned about the real threats of cyber fraud, child exploitation, and identity theft that international law obliges States to address. The trick is to reconstitute the Act in a manner that assures Pakistan will not trample fundamental freedoms in attaining causes that are legitimate in themselves. A doctrinally coherent reform agenda would find expression in possibly narrowing the ambit of offences regarding speech, introducing precise definitions, and directing defamation and reputation disputes to civil remedies. The powers of surveillance must be given prior judicial sanction with clearly defined limitations regarding scope and duration. The blocking and takedown regime must carry some procedural guarantees, such as immediate notification, appeal, and independent review (Khan, 2018).

Doctrinal Overview of the UK Investigatory Powers Act 2016

The Investigatory Powers Act, passed in 2016, is one of the most important pieces of surveillance regulation in England and Wales. The IPA was introduced to draw a line under existing investigatory powers, deal with the increasingly complex world around digital communications, and create a legislative framework for practice that, at the time of writing, had tended to be exercised under a mosaic of statutes or executive authority. Within the scope of the Act are interception of communications, equipment interference, acquisition and retention of communications data, bulk data powers, and technical capability notices with obligations imposed on service providers.

The industrial framework for IPA is vast and intricate in distribution. It also allows targeted interception warrants, giving intelligence agencies access to the contents of communications where doing so was necessary for national security, serious crime and economic well-being. It provides for equipment interference, under which agencies may acquire access to devices or networks to extract information. It governs retention and acquisition of communications data, including security metadata regarding when and how individuals communicate with one another. At the heart of contention even more is legitimization of bulk powers-attaching bulk interception and acquisition of bulk personal datasets (Cannataci, 2017).

One notable feature of the IPA is that it imposes a general duty of safeguarding privacy. The act does not make privacy a governing principle, but it requires decision-makers to take into account the need for safeguarding personal rights. The duty stands as recognition that surveillance should be exceptional rather than routine. Critics, however, contend that the framers of the general duty have thus far left it so wide in scope that only few criteria would bind it in such a

way as to have emanated from the state power itself (Glover, 2021).

From a human rights perspective, the most important issue in the doctrine is proportionality. Article 8 of the ECHR exemplifies the conditions under which interference in private life is legitimately pursued in terms stipulated by law with aims such as national security or crime prevention, and is deemed necessary in a democratic society. The European Court of Human Rights constructed detailed case law on these requirements, such that limitations on The law has to be accessible, intelligible, and foreseeable, and should contain adequate safeguards against abuse. The prescription upon freedom of expression as described under Article 10 must be finely formulated and subject to the highest degree of scrutiny, particularly when it concerns journalists and their confidential sources.(Victoria, 2018)

The law has passed through numerous challenges, and its substantive significance cannot be understood in isolation from case law. Civil society organizations such as Liberty, Privacy International, and Big Brother Watch have challenged the lawfulness of bulk powers, data retention, and protection of sensitive material. The framework has been largely upheld by domestic courts (including the Investigatory Powers Tribunal), albeit with some recognition of deficiencies in the safeguards. The Court of Justice of the European Union, prior to Brexit, found that the indiscriminate retention of data does not stand and that any measures for retention need to be targeted and with intense scrutiny.(Rab Nawaz, 2019)

The IPA has granted bulk powers that have posed some of the highest controversies. Bulk interception and bulk personal datasets collect enormous quantities of data, most of which pertain to individuals with no link to wrongdoing. This, doctrinally, raises grave issues under Article 8, with indiscriminate collection being at variance with the requirement of necessity and proportionality in surveillance. The government argues that bulk powers are needed to detect threats when, in a digital age, the identity of suspects may not be established in advance, and where highly sophisticated opposing forces are operating in a global communication system. Human rights doctrine (Cannataci, 2017).

In fact, the IPA has its own direct effects on Article 10's freedom of expression. Journalists, lawyers and many other professions which depend on confidentiality are at increased risks from the threat of having their communications intercepted. The Act adds stricter criteria for the examination to be carried out on any surveillance of journalistic material, but very early criticisms recorded that these safeguards were not strong enough in that agencies could access source material without independent prior approval. Further safeguards have been afforded after judicial criticism that require that Judicial Commissioners weigh the public interest in protecting journalistic sources in their warranty approvals.

The IPA direct effects freedom of expression under Article 10. Journalists and lawyers falling under professionals who depend on confidentiality suffer increased threats from interception of communications. The Act puts additional scrutiny into the application as concerns any surveillance of journalistic material, but already criticisms were expressed early that such safeguards were not strong enough, in that agencies could access source material without independent prior approval. Further safeguards have been afforded after judicial criticism that require Judicial Commissioners to weigh public interest in protecting journalistic sources during their warrant approvals (Glover, 2021).

In assessing the IPA frameworks against human rights standards, oversight and accountability become critical. The entire idea of IPCO was supposed to lend itself to very stringent auditing, inspecting, and reporting surveillance practices. The Investigatory Powers Tribunal now operates in parallel to IPCO, creating a judicial, specialized forum for those who believe that they have been unlawfully surveilled. These mechanisms, among others, speak to the UK's attempts to institutionalize oversight. However, doctrinal critiques point to their deficiencies. Although IPCO's reports are public, they are mostly generalized, lacking in details that could allow for meaningful public debate. The IPT often holds

hearings in private; thus, its actions are less transparent and limit the possibilities for individuals to contest surveillance effectively.(Gareth, 2018)

Doctrinally speaking, the assessment of the IPA raises strong and weak points. It supports the consolidation and clarification of investigatory powers while introducing judicial authorization and oversight structures, which would improve the fragmented and opaque framework of previous legislation. Authorization granted to generic powers, nebulous encryption, and partial interconnected safeguards for sensitive professional material continue to throw up tensions with respect to legality, proportionality, and effective remedy under ECHR.(Fiona, 2019)

Comparative Analysis: PECA vs IPA under Human Rights Standards

To date, the standards for cyberspace control and activities have been raised on everyone's priority list regarding national security and order with regard to human rights. The legislation poses two highly distinct experiences, leading to deep concerns regarding the application of laws to international human rights standards' motors - privacy, freedom of expression, due process, proportionality, and remedy. It illustrates that while rounds of PECA flounder under a wide ambit of authority challenged on concerns of vagueness and political abuse, IPA moves with a refined architecture, independent entities, and judicial constraining checks, leaving it exposed to accusations stemming particularly from bulk-surveillance powers and implications on encryption.

In Pakistan, under the cyber laws promulgated in 2016, work is underway for the development of an elaborate compendium for cybercrime investigation and prosecution. The law provides for the punishment of an incredible number of crimes, varying from hacking and data interference to crimes pertaining to information and communication technologies. Furthermore, a plethora of other content-based offences have also been tucked in, including cyber harassment, impersonation, defamation, and the spreading of "false information." Such provisions have been framed rather broadly and generally vaguely, making them prone to arbitrary enforcement. The later amendments that are chiefly discussed in 2021 and completed in 2025 increased government powers to regulate platforms, demand messages be traceable, and a ban on any content that the government deems unlawful. Critics assert that the vague nature of these offences threatens legitimate speech, creates chilling effects for journalists and activists, and fails the human-rights test of foreseeability. By contrast, the United Kingdom's Investigatory Powers Act of 2016 is different in structure. This Statute is primarily enabling legislation giving investigative authorities powers to intercept communications, retain data, do equipment interference (commonly understood as lawful hacking) and in some cases conduct bulk data collection.(Madiha, 2020)

The other area plainly in which these two statutes contrast in abundance is that of oversight. Under the PECA, the Swedish Federal Bureau of Investigation (FIA)-type organizations have investigatory powers, including the ordering of takedown notices and access to user data. Rarely does known independent judicial review exist. By contrast, the practice is erratic and highly unpredictable and gives the executive leeway. There are hardly any transparency mechanisms available; hence the little reporting that has been done on the number of takedown orders, preservation requests, or prosecutions.

Advocates for human rights maintain that a considerable jurisdictional void for creating a misuse of this law has arisen. In other words, the IPA created the investigatory Powers Commissioner's Office (IPCO) under an act of Parliament in order to oversee the exercise of surveillance powers. IPCO audits the agencies and reports annually to Parliament on the number of warrants approved, rejected, and errors made in granting them. Furthermore, for the most intrusive powers, independent judicial approval is required by the "double-lock" system.(Huma, 2021)

Another irony in human rights revolves around data retention and bulk powers, including encryption. The 2025 amendments of PECA now enforce the obligation on the part of platforms to trace the originators of messages and keep user data which would then be provided to authorities when they

request. Local digital rights organizations contend such traceability would destroy the end-to-end encryption and thus jeopardize the safety of their private conversations.

By catalogue and detailed definition, bulk powers within the IPA are more apparent: bulk interception, bulk acquisition of communications data, and bulk equipment interference are now allowed with the issuance of warrants. For their part, UK authorities have defended these powers as being necessary within the context of national security. However, rights advocates argue that such blanket collection of data compromises the privacy rights of individuals having little connection to crime or terrorism. It is also the law under IPA that compels an authority to force service providers to give "assistance," interpreted as potentially obliging them to soften encryption. Such provisions have been warned by Amnesty International and other NGOs to create global dangerous precedent. International standards provided by the UN Human Rights Committee stress that data collection should be targeted, scoped to that particular situation, and for a limited time, before subjected to independent oversight.(Ellen, 2018)

The differing implications of the two regimes relate to freedom of expression and press freedom. Journalists and civil society activists in Pakistan and opposition figures have spoken of an immediate effect from PECA. In particular, the HRCP has documented that the vague provisions of the Act are set up as devices to suppress political dissent, remove critical content, and prosecute individuals for defamation, or for allegedly spreading "disinformation." Self-censorship online is the clear result: fear of penalty induces citizens to fear legal consequences and so self-censor. The IPA in the UK does not directly criminalize expression; it is rather an indirect inference of the impact it has on expression through awareness of intercepted or retained communications. There are protections for journalistic sources; additional authorization would have to be secured for targeting material related to journalism. Right advocates argue that the bulk surveillance jeopardized the confidentiality of sources, and the law has faced litigation on this basis.

The transparency and public accountability that the two systems exhibit, however, separate the two. Pakistan has not yet made it a point to institutionalize regular public reporting on what would look like the taking up of powers under PECA. Most data on takedowns, any prosecutions, or errors is intermittent, collected under pressure or in bits and pieces. The opacity denies accountability and public debate about the law's proportionality. In the UK, the requirement is statutory reporting to IPCO under the IPA, and many of their annual reports contain aggregated statistics on the warrants issued and compliance problems. Critics want more granular statistics, but the existence itself of a mandatory reporting regime is a safeguard.(Michael, 2019)

Evidently, that is true. PECA would definitely benefit from a cut-and-dry narrowing and clarification of offences inside its legislation, especially where the ones about speech should probably be imprecise and redrafted to ensure that they are fit for legality, necessity, and proportionality. An independent oversight authority modelled on the Investigatory Powers Commissioner of the United Kingdom should be created with powers to audit agencies, publish reports, and investigate complaints: Intrusive measures like interception or compelled decryption should call for independent judicial authorization and not just executive discretion. Such measures would create an institutionalized requirement for disclosure in statutory reports. Last but certainly not least, remedies should be put in place to ensure that the individual can access redress mechanisms in the event of a violation of his/her rights.

Empirical and Practice Insights

The comparative empirical and experiential insight of PECA and IPA in relation to personal privacy, proportionality, transparency, and remedies against the international human rights framework. I examined laws in operation in terms of institutional actors, evidence of administrative abuse or

administrative safeguards, judicial and independent oversight, and real-life effects on journalists and ordinary users that these would have on compliance with human rights norms.

The offences under PECA, framed very widely using vague words, criminalise expressions that serve to chill dissent and intimidate known journalists and human rights defenders in Pakistan, but independent analyses find PECA procedural safeguards-warrants, judicial oversight, and challenge avenues-weakened in practice. Its operational authorities have also been given huge discretionary powers for accessing user data and demanding blocking of content-very often through administrative rather than court orders-thus creating an glaring asymmetry in access to remedies for ordinary citizens. News stories of shocking FIRs, summons, and arrests made under PECA's defamation, anti-terror, and fake news provisions illustrate how the criminal tools of this law become instruments of content control because of weak prosecutorial independence and institutional checks. They throw the necessary and proportionate principles it must observe into disarray, hence violating international human rights standards.(Laura, 2017)

Apart from the irrational gaps acknowledged by law, investigators on the frontline and service providers often do not have a clear understanding of lawful interception standards, retention limits, and data-minimization obligations; hence these laws are being applied uniformly, leaving opportunities for over-collection of personal data. In short, while PECA gives the State clear operational advantages for the purpose of investigating electronic crimes, academics and civil society audits would argue that these very advantages, such as vagueness in prohibited content, administrative routes of access, and limited meaningful oversight, routinely pose a risk to the human rights of privacy and free expression in Pakistan.(Rabia, 2021)

It was an act in the UK that aimed at codifying, centralizing and arguably strengthening legal safeguards towards interception, bulk data and equipment interference; in practice, it gave a much more developed architecture of warrants, independent oversight through the offices of the Judicial Commissioner and statutory reporting obligations. Empirical oversight reports, along with the post-implementation review, indicate that there have been tangible steps toward improvement in audit, the formalization of a "double lock" for certain warrants, and building institutional capacities for oversight that are generally lacking in the majority of other jurisdictions, but those improvements have yet to take away from the existing legal frameworks and consequences (Cannataci, 2017).

Parts of the UK regime have repeatedly proven hard to reconcile with civil society litigants and the courts against human rights standards: guidance and remedial orders have been needed to address incompatibilities (for example around special safeguards for journalistic material in bulk interception), and recent high-profile litigation (including industry challenges over encryption and Technical Capability Notices) demonstrates the frictions between operational surveillance tools and rights to confidentiality and press freedom. Empirical monitoring shows that UK agencies typically do employ warrant processes and engage in oversight reporting, but the system still struggles with an undercurrent of secrecy (closed hearings, redaction of oversight reports), broader definitions of bulk powers, and intrusive investigatory techniques such as equipment interference and compelled decryption. They show different overall practical outcomes; thus, with a stronger procedural scaffolding, it will have something to do with providing lawful remedy and audit in the UK-an important element for human rights compliance-but continued challenges in court and political debates show that much architecture does not guarantee on-ground outcomes will remain proportionate.(Farah, 2020)

Comparative lessons from practical experience suggest three closely held and actionable conditions to bring either regulatory system in alignment with international human-rights standards: (1) clear legal thresholds: the laws must specify precisely when data may be accessed, by whom and with what judicial or quasijudicial authorization; vague offences or administrative shortcuts may simply be a means of

arbitrarily enforcing the law; (2) meaningful oversight and transparent public accountability, run by independent agencies which are enabled to inspect, report publicly for public accountability except for genuine national security concerns, and trigger remedial action; without depth and visible transparency, statute-based guarantees will only remain on paper; and (3) Clear systems, keeping areas of risk to a minimum, and establishing high protections under law for redemption and safety for intermediaries and victims means users, journalists and platforms must have fast, inexpensive methods to query such orders, with robust regulations on requests relating to data minimization, retention limits, and destruction of compromising data.(Jonathan, 2018)

Empirical audits indicate that the UK comes out on top due to procedural checks and institutionalization of oversight but does fail basic ECHR/ECtHR tests, failing to provide for strong remedial orders or the opportunity to litigate them. PECA in Pakistan enjoys wide-enabling enforcement powers but does not provide for consistent independent oversight, and its workings have already been called out for putting a chill on free expression and putting journalistic work at risk, according to rights watchdogs.

Conclusion

A comparative analysis of the Prevention of Electronic Crimes Act (PECA) 2016 of Pakistan and the Investigatory Powers Act (IPA) 2016 of the United Kingdom shows that the two measures are purporting to strike a very fine balance between state security considerations and personal privacy under human rights standards. Both laws were meant to protect against threats from cyberterrorism and other forms of digital crime, but they take on completely different forms. In Pakistan, PECA 2016 has been under serious scrutiny for its broad and vague provisions allowing for extensive powers, mainly to law enforcement, without sufficient judicial checks. The law raises major concerns about arbitrary surveillance, stifling of freedom of expression, and encroachment upon the privacy rights of citizens guaranteed under the Constitution of Pakistan as well as by international obligations like the ICCPR. Although the IPA 2016 of the United Kingdom has been referred to alternatively as "snoopers' charter," it indeed carries a relatively stronger regime of checks and balances in terms of dual authorization (executive and judicial commissioners), restrictions on data retention, and proportionality requirements which are much cleaner with the standards of the European Convention on Human Rights.

In balancing national security and civil liberties, both regimes bear the brunt of some indications of possible human rights violations. To its credit, the erstwhile regime at least tried in a somewhat structured manner to provide for some oversight mechanisms, albeit not perfectly designed. The peculiarities of Pakistan presented far greater challenges to the institutional safeguards and judicial scrutiny that are absent, and the PECA never had a data protection law to strengthen it. Surveillance practices in Pakistan therefore tend to run a risk of disproportionate violations under the Freedom of Speed, affecting journalists, political activists, and dissenters most adversely and thus hampering democratic accountability.

References

Aleem, Y., Asif, M., Khaliq, M., Imtiaz, I., & Ashraf, M. U. (2023). The Prevention of Electronic Crimes Act 2016 and shrinking space for online expression in Pakistan. *Elementary Education Online, 20*(2), 1019–1026. https://doi.org/10.17051/ilkonline.2021.02.114
Google Scholar Worldcat Fulltext

Cannataci, J. A. (2017). *Report of the Special Rapporteur on the right to privacy* (Human Rights Council document). United Nations Office of the High Commissioner for Human Rights. https://ccdcoe.org/uploads/2018/11/UN-170224-AHRC3460.pdf
Google Scholar Worldcat Fulltext

Glover, P. (2021). *Protecting National Security: A History of British Communications Investigation Regulation*. Routledge.
Google Scholar Worldcat Fulltext

Government of Pakistan. (2016). *Prevention of Electronic Crimes Act, 2016* [Act No. 21 of 2016]. National Assembly of Pakistan. https://www.na.gov.pk/uploads/documents/1470910659_707.pdf
Google Scholar Worldcat Fulltext

Iqbal, M., Raza Talpur, S., Manzoor, A., Abid, M. M., Shaikh, N. A., & Abbasi, S. (2023). The Prevention of Electronic Crimes Act (PECA) 2016: Understanding the challenges in Pakistan. *Siazga Research Journal, 2*(4), 273–282. https://doi.org/10.58341/srj.v2i4.35
Google Scholar Worldcat Fulltext

Karabacak, B., Yildirim, S. O., & Baykal, N. (2016). Regulatory approaches for cyber security of critical infrastructures: The case of Turkey. *Computer Law & Security Review*, *32*(3), 526–539. https://doi.org/10.1016/j.clsr.2016.02.005
Google Scholar Worldcat Fulltext

Khan, E. A. (2018). *The Prevention of Electronic Crimes Act 2016: An analysis*. Shaikh Ahmad Hassan School of Law, Lahore University of Management Sciences (LUMS). https://sahsol.lums.edu.pk/node/12862
Google Scholar Worldcat Fulltext

Looney, S. (2025). Avoiding the Thin Veneer of Legality; Structural and Institutional Factors Impacting Judicial Scrutiny in a National Security Context. *Liverpool Law Review, 46*(2), 245–269. https://doi.org/10.1007/s10991-025-09385-1
Google Scholar Worldcat Fulltext

Milanovic, M. (2018). Human rights treaties and foreign surveillance: Privacy in a digital age. *Harvard International Law Journal, 59*(1), 81–146. https://harvardilj.org/wp-content/uploads/sites/15/2018/02/HILJ_59-1_81_Milanovic.pdf

Murphy, M. H. (2015). Surveillance and the right to privacy: Is an 'Effective remedy' possible? In *Springer eBooks* (pp. 289–306). https://doi.org/10.1007/978-3-319-24016-9_12
Google Scholar Worldcat Fulltext

Nawaz, R. (2019). Legislative drafting and ambiguity: Problems in PECA's language. *Karachi University Law Review, 2*, 119–140.
Google Scholar Worldcat Fulltext

Tariq, H. (2021). Human rights litigation in Pakistan: Privacy claims under constitutional jurisprudence. *Pakistani Journal of Constitutional Law, 13*, 97–122.
Google Scholar Worldcat Fulltext

United Kingdom. (2016). *Investigatory Powers Act 2016* (c. 25). https://www.legislation.gov.uk/ukpga/2016/25/contents
Google Scholar Worldcat Fulltext

Wetzling, T., & Vieth, K. (2021). Legal safeguards and oversight innovations for bulk surveillance. In *Routledge eBooks* (pp. 145–164). https://doi.org/10.4324/9781003120827-11
Google Scholar Worldcat Fulltext

White, M. (2024). *Surveillance Law, Data Retention and Human Rights: A Critical Analysis*. Routledge.
Google Scholar Worldcat Fulltext