

PRIVACY IN PERIL: THE ROLE OF INTERNATIONAL LAW IN REGULATING DIGITAL SURVEILLANCE IN THE 21ST CENTURY

Ali Shahid

Lecturer in Law, Grand Asian University, Sialkot, Pakistan
Ali.shahid@gaus.edu.pk

Dr. Usman Hameed

Professor of Criminology at University of Lahore
usman.hameed@crim.uol.edu.pk

Arfan Ahmad

Lecturer in Law, Premier Law College, Gujranwala. Senior Law Officer, Chaudhary Pervaiz Elahi Institute of Cardiology, Wazirabad.
arfanahmd10@gmail.com

ABSTRACT

The rapid expansion of digital technologies has empowered states to conduct pervasive surveillance, placing privacy at risk worldwide. This article examines how international law constrains (or fails to constrain) digital surveillance, with a focus on Pakistan and a comparative look at the European Union. International instruments such as the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR) affirm the right to privacy; recent UN resolutions (e.g. HRC Res. 54/21 of 2023) extend these protections to the digital age. However, many states struggle to implement these norms. In Pakistan, Article 14 of the 1973 Constitution explicitly declares that the “dignity of man” and “privacy of home” are inviolable, and the Supreme Court has denounced unauthorized wiretapping as “illegal, immoral and unconstitutional”. Yet Pakistan’s legal framework includes colonial-era laws (e.g. Telegraph Act 1885, updated by the 1996 Telecommunication Act), and new statutes (e.g. the Prevention of Electronic Crimes Act 2016 and the Fair Trial Act 2013) whose broad powers have outpaced effective oversight. Recent events – such as the 2024 revelation of a nationwide telecom surveillance system (LIMS) and the introduction of a draft Personal Data Protection Bill – underscore how gaps in law and enforcement can enable mass surveillance. By contrast, the European Union combines strong data-protection norms (GDPR, Charter of Fundamental Rights) with evolving law-enforcement rules, although it too grapples with balancing security and privacy (as seen in 2025 EU proposals on data retention). This article traces these developments, analyzes enforcement challenges, and offers reform recommendations: Pakistan must enact and enforce a robust data protection

regime, tighten judicial oversight of interception, and align its laws with international standards. It also reflects on the future of privacy under international law: while current norms reaffirm digital privacy rights, the gap between law and practice points to the need for stronger global governance and accountability mechanisms to protect personal freedom in the digital age.

Keywords: International Law, Human Rights, Privacy Violations, State Responsibility, Global Governance, International Legal Instruments

Introduction

Advances in information and communication technologies have made digital data collection ubiquitous. Governments worldwide now deploy sophisticated systems – from internet traffic monitoring to biometric databases – that can intrude on individuals’ private lives. The United Nations has emphasized that human rights norms must follow people online as well as offline, noting that “the same rights that people have offline must also be protected online, including the right to privacy”. (Ionita, C. V., & Kanetake, M. 2023) Yet the legal regulation of surveillance is highly uneven. In many countries, domestic legislation and practice lag behind the international commitments that they have undertaken. As Privacy International has observed, forms of mass surveillance used by governments “directly threaten the very core” of the right to privacy. (Zaki abbas, 2024) This creates serious human rights implications, especially for vulnerable groups (journalists, minorities, dissidents) who may be disproportionately targeted by indiscriminate monitoring. (Dror-Shpoliansky, D., & Shany, Y. 2021)

This article analyzes how international law addresses digital surveillance, focusing mainly on Pakistan and comparing it to the European Union. Pakistan is an illustrative case: on paper it recognizes privacy as a constitutional and treaty-based right, but in practice its security agencies have broad powers and lack transparency. In contrast, the EU has developed detailed privacy and data-protection laws, even as member states adapt to new security challenges. The structure is as follows. After defining key terms in Section II, Section III reviews the international legal framework – from the Universal Declaration of Human Rights (UDHR) and International Covenant on Civil and Political Rights (ICCPR) to recent UN Human Rights Council resolutions and the UN Special Rapporteur’s mandates. Section IV examines Pakistan’s own legal framework and case law on surveillance, highlighting constitutional guarantees, statutes, and judicial rulings. Section V compares this with the European context (drawing on EU law, the EU Charter of Fundamental Rights, and case law). Section VI surveys recent developments (2023–2025) that illustrate the current state of play: for Pakistan this includes revelations of mass interception systems and the passage of draft data-protection legislation, while for the EU this encompasses new policy proposals on access to data. Section VII identifies key enforcement challenges and gaps under international and domestic law. Section VIII offers recommendations for reform, both for Pakistan and at the global level. Finally, Section IX concludes by reflecting on the future of privacy protection in the digital era under international law. Throughout, we cite authoritative sources – including legal texts, UN reports, judicial decisions, and expert analyses – to substantiate the discussion.

Background and Definitions

The right to privacy is a long-recognized human right, but its scope in the digital age requires clarification. “Privacy” generally refers to the right of individuals to control access to their personal information and to be free from arbitrary intrusions into their private and family life. In the words of the UN Human Rights Council, no one should suffer “unlawful interference” with their privacy, family, home or correspondence. (Shaelou, S. L., & Razmetaeva, Y. 2023) Privacy is linked to personal autonomy, dignity, and freedom of expression; when people know they are being watched, a chilling effect can deter free speech and assembly. (P L D 1998 Supreme Court 388) Digital surveillance encompasses any state-sponsored (or private) collection and analysis of electronic data about individuals. It ranges from targeted wiretapping of suspects’ phone calls to indiscriminate mass collection of metadata, as well as location tracking, internet monitoring, facial recognition cameras, and biometric identification. Such technologies can include internet and phone “packet capture,” subscriber data recording, real-time interception, and algorithmic analysis of big data. Crucially, digital surveillance often blurs the line between public and private spheres, since people routinely use networks and services that can be monitored outside the confines of their homes.

Data protection is a related but distinct concept. It refers to legal rules governing the processing of personal data – i.e. any information relating to an identified or identifiable person. Data-protection laws (like the EU’s General Data Protection Regulation) aim to ensure that data collected by both governments and private companies are handled lawfully, with individuals’ consent or a legitimate ground, and with security safeguards. In practice, surveillance often raises data-protection concerns when intercepted communications or records are stored and shared without adequate protections. For this article, “digital surveillance” is used broadly to include both intelligence-gathering by state agencies (telecommunications intercept, internet monitoring, CCTV, drones, etc.) and associated data collection and retention practices that implicate privacy rights.

This article adopts the perspective of international human rights law, in which the right to privacy is subject to certain lawful restrictions (for example, for national security) but must always be “necessary and proportionate”. (Psychogiopoulou, E.2024) International norms do not accept blanket or secret surveillance without safeguard. A key international definition is found in ICCPR Article 17, which states that “no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence” and that everyone has the right to protection of the law against such interference. This means any surveillance must be authorized by law, aimed at a legitimate purpose (e.g. serious crime), and accompanied by independent oversight. In *Klass v. Germany* (European Court of Human Rights, 1978) and later cases, Europe’s judges similarly held that state interception requires clear legal bases and controls to prevent abuse. In sum, while the term “digital surveillance” is not explicitly defined in treaties, it is governed by the general privacy standards set forth in international human rights instruments and interpreted by treaty bodies and courts to include protection against intrusive government monitoring. (ICCPR)

International Legal Framework

International human rights law provides a framework affirming the right to privacy. Although the UDHR (1948) is not itself a binding treaty, it proclaims in Article 12 that “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence”. (Sahar Iqbal, 2023) This clause underpins the more binding obligations in the ICCPR (1966), to which Pakistan and many states are parties. Article 17 of the ICCPR explicitly prohibits arbitrary or unlawful privacy interferences and guarantees protection by law against such acts. Importantly, the UN Human Rights Committee (the ICCPR monitoring body) has clarified in general comments (e.g. GC16) that surveillance programs must not be “arbitrary,” meaning they require clear legal authority, legitimate aims, proportionality, and independent oversight. Pakistan ratified the ICCPR in 2010, obligating it to respect these standards. Other treaties also echo privacy rights: for example, Pakistan is party to the Convention on the Rights of the Child (Article 16) and the Cairo Declaration on Human Rights in Islam (Article 18), both safeguarding personal privacy. These international instruments affirm that privacy is fundamental and that member states, including Pakistan, are duty-bound to uphold it. (Sahar Iqbal, 2023)

The European human rights system likewise enshrines privacy in Article 8 of the European Convention on Human Rights. The European Court of Human Rights (ECtHR) has held that secret surveillance without sufficient safeguards violates Article 8 (e.g. *Zakharov v. Russia* (2015), *Big Brother Watch v. UK* (2021)). In the European Union, the Charter of Fundamental Rights (binding on EU institutions and member states) explicitly includes the “right to respect for private and family life” (Article 7) and the “right to protection of personal data” (Article 8). (Eeckhout, P. 2002) The EU’s General Data Protection Regulation (GDPR) and related directives (e.g. for law enforcement) translate these rights into detailed requirements, limiting how governments and companies can use personal data. In particular, data must be collected for specified, legitimate purposes, retained only as long as necessary, and protected by security measures. The GDPR also requires that data subjects have rights of access, correction, and redress. Although the GDPR mostly regulates private processing, it sets a high European standard for handling personal information that also influences how state surveillance data must be treated.

At the United Nations, the right to privacy in the digital age has recently drawn focused attention. In 2015 the UN Human Rights Council created the mandate of the Special Rapporteur on the right to privacy (first held by Joseph Cannataci), recognizing that global surveillance, new technologies, and transnational data flows present new challenges to privacy rights. Cannataci’s mandate (and now that of his successor) includes reviewing state surveillance laws worldwide and advising on human rights-compliant practices. Human Rights Watch noted that the mandate was intended to address the “increasingly imperiled right to privacy” and its link to freedom of expression and democracy. The Special Rapporteur has issued reports on topics like mass surveillance, encryption, and biometric data, stressing principles such as necessity, legality, and proportionality in any surveillance regime. For instance, the UN has noted that pervasive digital monitoring can chill dissent and restrict free assembly, and has urged clear rules and transparency in intelligence work. (Custers, B. 2022)

Most recently, the UN General Assembly and Human Rights Council have adopted resolutions specifically on “Privacy in the Digital Age.” In October 2023 HRC Resolution 54/21 reaffirmed that privacy is intrinsic to human dignity and democracy, and it called on states to prohibit certain intrusive technologies (e.g. blanket facial recognition in public spaces) and ensure that biometric mass surveillance is compatible with human rights. The resolution explicitly recognized that “automated data processing and profiling” can violate privacy, and it urged governments to develop safeguards against unauthorized digital monitoring. While UN resolutions are not legally binding, they signal a growing international consensus: they insist that the same privacy rights enjoyed offline must be protected online, and they urge member states (including Pakistan) to ensure surveillance laws respect human rights. (UN General Assembly, 2023)

In short, international law – through treaties, judicial bodies, and UN mandates – requires that digital surveillance be limited by law, necessary for a legitimate purpose, and subject to oversight. Arbitrary or secret mass surveillance is inconsistent with human rights norms. The next sections examine how Pakistan’s domestic framework compares to these standards, and what insights can be drawn from the EU’s approach. (Psychogiopoulou, E. 2024)

Domestic Legal Framework in Pakistan

Constitutional Rights and Jurisprudence

Pakistan’s Constitution (1973) expressly recognizes privacy. Article 14(1) declares that “the dignity of man and, subject to law, the privacy of home, shall be inviolable”. This is a notably strong formulation: the phrase “inviolable” suggests that privacy is a fundamental guarantee. Indeed, as Privacy International observes, Article 14 was intended to take precedence over ordinary laws (although its protection is “subject to law,” meaning the legislature may impose restrictions). The Supreme Court of Pakistan has interpreted Article 14 broadly. In the landmark *Benazir Bhutto v. President* case (1997), the Court held that surreptitious telephone-tapping and eavesdropping violated the “dignity of man” and the “privacy of home,” injuring personal honor and placing individuals in danger of blackmail. It famously ruled that telephone conversations are constitutionally protected and that any such interception could only be justified (if at all) in cases of defence or national security. (Article 14, Constitution of Pakistan 1973) The Court even directed that in the absence of a specific law on surveillance, any future wiretapping must be authorized only by the Supreme Court or a court-appointed commission for limited periods. The judgment declared unauthorized surveillance to be “illegal, immoral and unconstitutional”. In sum, early jurisprudence set a high bar: Article 14 covers an individual’s privacy “wherever he lives or works,” not just inside the home, and any state intrusion requires strict legal authority and review. (P L D 1998 Supreme Court 388)

Since *Benazir*, Pakistani courts have reiterated that privacy extends beyond just the four walls of one’s house. For example, a 2018 Supreme Court case found that even property records in a public registry cannot be accessed without due process, as to do so would violate privacy and dignity. Another decision emphasized that telephone conversations are not available for arbitrary surveillance. Although there have been few recent landmark privacy rulings, these precedents establish that Pakistan’s highest

courts acknowledge privacy as a fundamental right interlinked with other freedoms (speech, life and liberty).

At the same time, the Constitution provides some exceptions. Article 8 permits laws to infringe rights if needed for armed forces' "proper discharge" of duties, which has been interpreted broadly. Moreover, Article 4 declares that each Pakistani has the duty to protect the Constitution and the law. Together, these clauses could be argued to authorize certain security laws. However, article 14 remains the core privacy guarantee, and the constitution also has Article 25 (equality) and Article 19 (freedom of speech) which have been linked to privacy (for instance, courts have noted that phone tapping can also violate free speech rights).

Statutory Framework and Agencies

Pakistan's surveillance powers stem from a patchwork of laws, some dating to the British colonial era. The Telegraph Act of 1885 initially gave the government power to intercept telegraph and telephone communications during "emergencies." It was later supplemented by the Pakistan Telecommunications (Re-organisation) Act, 1996 (a.k.a. the PTA Act), which allows the federal government to authorize individuals or agencies to intercept or monitor communications for state purposes. Although these older laws required warrants for taps, enforcement was lax and oversight weak. (Sahar Iqbal, 2023)

More recently, Pakistan has enacted new statutes governing electronic data. The Investigation for Fair Trial Act of 2013 is a landmark: it permits investigators to access stored communications (emails, phone calls, text messages, and other electronic data) only with a warrant issued by a High Court judge. This law, passed after years of debate, was designed to align surveillance with due process. In theory, it requires a judicial determination that surveillance is necessary for a defined criminal investigation before any interception or data access can occur. Similarly, the Prevention of Electronic Crimes Act (PECA) 2016 – part of the post-2014 "National Action Plan" on terrorism – criminalizes various cyber offenses but also grants sweeping surveillance authorities. PECA allows the Pakistan Telecommunications Authority (PTA) to block or remove online content (including for vague reasons such as "public order" or national security). Crucially, PECA's Section 36 permits "real-time collection and recording" of data if a court is satisfied that the information is required for a criminal investigation. This in effect creates a mechanism for live interception, albeit nominally under court order. PECA further encourages data sharing: Section 39 even allows sensitive personal data to be shared with foreign agencies around the clock. Human rights groups have criticized PECA's broad terminology (e.g. undefined "national security" grounds) as weakening privacy and free speech. (PECA Act, 2016)

In addition, the Monitoring and Reconciliation of Telephony Traffic Regulations (2010) require telecom companies to install systems for *real-time monitoring and logging of all telephone network traffic*. In practice, this created the *Lawful Intercept Management System (LIMS)* mandated by the PTA. As investigators revealed in 2024, LIMS allows agencies to tap into live phone and internet data of any user, up to 2% of all subscribers at a time, without any court approval. In other words, the state built a mass-surveillance infrastructure through these regulations, effectively banning

encryption and placing confidentiality of communications at risk.

Pakistan's intelligence and security agencies – notably the Inter-Services Intelligence (ISI) and Military Intelligence – also operate under their own legal powers (such as the ISI Act of 1972). These are largely opaque. In effect, a citizen's digital life may be subject to interception by multiple agencies, some under judicial warrant (Fair Trial Act) and others under executive authorization (Telecommunications Act) with minimal transparency. Critics note that Pakistan has *no comprehensive data protection law* to constrain either state or corporate use of personal data, though a Personal Data Protection Bill has been drafted (see below). In sum, while Pakistan has nominal legal checks (warrant requirements) and constitutional guarantees, actual surveillance practice has often proceeded under broad older laws with little independent oversight.

International Obligations and Recent Challenges

As mentioned, Pakistan has ratified key human rights treaties. Under the ICCPR it must respect Article 17; under the Convention on the Rights of the Child it must protect children's privacy. It is also a party to the ICCPR's Optional Protocols and the Universal Periodic Review process, which has repeatedly urged Pakistan to reform its surveillance laws. In practice, however, surveillance has sometimes operated "arbitrarily." For example, in 2023 the Islamabad High Court found that telecom operators had been enabling LIMS-based surveillance on government orders, without any court warrant or public disclosure. Justice Babar Sattar noted that *no* executive authorization was recorded for this sweeping interception. The court temporarily barred agencies from using LIMS without following the *Investigation for Fair Trial Act's* warrant procedure, under penalty of violating fundamental rights. This episode illustrates the gap between international commitments and reality: Pakistan's leadership must now ensure that its agencies truly adhere to lawful processes, or else face judicial rebuke. (Malik Asad, 2024)

In summary, Pakistan's domestic framework presents both promise and peril. Its Constitution and superior courts emphasize privacy, yet its surveillance infrastructure (old statutes, telecom regulations, and new anti-terror laws) has expanded rapidly, often ahead of democratic checks. The result has been an environment where privacy can be overridden for vague security goals. The next section examines how other jurisdictions grapple with similar issues, to draw comparisons.

Comparative Legal Framework (European Union)

Comparing Pakistan to another jurisdiction highlights both common issues and alternative solutions. We focus on the European Union, which has developed a comprehensive (if evolving) privacy regime. EU law differs from Pakistani law in that it explicitly treats privacy and data protection as fundamental rights. The Charter of Fundamental Rights of the EU (binding on EU institutions and member states) includes Article 7 ("respect for private and family life") and Article 8 ("protection of personal data"). These rights are enforceable in EU courts. EU legislation translates these rights into concrete rules: the General Data Protection Regulation (GDPR) sets uniform standards for how personal data may be collected and used by any organization in the EU (including government). It embodies principles of lawfulness,

purpose limitation, necessity, and security of data processing. Another law enforcement instrument, Directive (EU) 2016/680, governs how police and judicial authorities handle personal data. Additionally, the ePrivacy Directive (soon to be replaced by an EU Regulation) specifically safeguards the confidentiality of communications by prohibiting interception of electronic messages or usage data without legal basis and safeguards. In short, EU law requires explicit legal authorization for any surveillance or data access, with oversight by courts or independent authorities. (Kellerbauer, M., Klamert, M., & Tomkin, J. 2024)

The European Court of Justice (CJEU) and European Court of Human Rights (ECtHR) have curtailed blanket surveillance schemes in Europe. Notably, in *Digital Rights Ireland* (2014) the CJEU struck down the EU Data Retention Directive because it mandated mass retention of telephony metadata for all citizens, violating the proportionality principle. Subsequently, in *Tele2/Watson* (joined cases C-203/15 and C-698/15, 2016) the Court held that EU law does not prohibit targeted retention of traffic and location data by member states, *provided* it is accompanied by adequate safeguards and limited to specific objectives (such as investigating serious crime). The ECtHR echoed this logic in *Big Brother Watch v. UK* (2021), finding that indiscriminate retention of communications data by UK authorities lacked sufficient limits and oversight. In effect, both European bodies demand that any state surveillance measure be necessary in a democratic society and subject to independent review. (Lubin, A. 2022) As a summary by the European Parliament's research service notes, "CJEU case law has set detailed requirements for data retention" – in particular, *only general and indiscriminate retention of traffic and location data for all users is permitted solely in the interest of national security; targeted retention may be allowed for public security or other important public interests, and even then with "robust safeguards"*.

In practice, EU member states implement these rules in national law. Many countries now require law enforcement to obtain judicial warrants for intercepting communications, similar to Pakistan's Fair Trial Act. For example, several EU countries have specific provisions that only a judge may authorize wiretaps, and legislative oversight committees review intelligence activities. However, EU states also seek new surveillance powers in the face of modern threats. Notably, in 2023–2024 the European Commission adopted an internal security strategy which includes plans for "effective access to data by law enforcement". A 2025 EU "Roadmap" proposes updating data retention rules to accommodate law enforcement needs while respecting CJEU precedents. The Commission acknowledges that any new EU retention law must comply with the strict CJEU standard that obligations be "strictly necessary" and not general or indiscriminate. It also proposes measures for cross-border interception cooperation and for technical access to encrypted data (by supporting decryption tools rather than banning encryption). These debates illustrate the tension even in Europe between security and privacy. (Paul Maynard, 2025)

Another EU development is the proposal of an AI Act (2021–2023). The Act would ban remote biometric identification (face recognition) in public spaces when used by law enforcement, calling it "high risk" and fundamentally incompatible with the right to privacy in a democracy. This mirrors the UNHRC's call to prohibit such technologies. If adopted, the EU AI Act would legally restrain one of the most

controversial surveillance tools. (Ebers, M. 2023)

Overall, the EU's comparative regime emphasizes individual rights and data protection. Unlike Pakistan, EU citizens generally have explicit statutory rights over their data (access, correction, etc.) and binding oversight mechanisms (Data Protection Authorities). Enforcement is not perfect – intelligence programs still exist (e.g. some countries' bulk metadata logging) – but failures are often challenged in court. In summary, the EU framework illustrates a model where privacy is treated as a fundamental right balanced against security: any encroachment on privacy must be carefully justified, narrowly tailored, and subject to accountability (the “proportionality” test).

Recent Developments (2023–2025)

The past two years have seen significant news in Pakistan and internationally that bear on surveillance and privacy.

Pakistan:

In mid-2023 and 2024 Pakistani courts and media exposed the extent of digital surveillance. In particular, the Islamabad High Court uncovered that the Pakistan Telecommunication Authority (PTA) had mandated all telecom operators to deploy a *Lawful Intercept Management System (LIMS)* connected to a centralized “surveillance centre.” Through LIMS, any agency could trace, intercept, and copy the communications of any phone or internet user. A court order described how, “without any human intervention,” the system would automatically retrieve the full content of voice calls, SMS, browsing history and other data for any targeted SIM or device. The order warned that 2% of all subscribers (about 4 million people at any time) could be monitored through this mass-surveillance infrastructure. These revelations drew sharp criticism from digital rights activists. Nighat Dad (citizen rights lawyer) noted that telecom companies had failed to be transparent with their customers, and argued that privacy-protective remedies do exist: aggrieved users could sue companies for violating their Article 14 privacy rights. Media Matters co-founder Sadaf Khan pointed out the irony that Pakistan lacks any comprehensive data protection law, meaning LIMS's existence had no legal barrier. The court's comments underscored that agencies had in effect bypassed the Fair Trial Act's warrant process by simply demanding data through the LIMS mechanism. As Justice Sattar observed, “*neither PTA nor the telecom companies shall authorize... any surveillance or interception of phone calls or data*” except under duly issued High Court warrants. In July 2024 the IHC clarified that telecom operators are no longer allowed to pass on call records or location data to police without judicial authorization, partially lifting a broad 2023 ban on sharing data. (Kemal, et al 2024)

Legislatively, Pakistan has moved on data protection. In May 2023 the Ministry of IT published a draft Personal Data Protection Bill. Civil society groups (and Privacy International) criticized the process as opaque: the government approved the draft without public consultation. The draft contains concerning clauses: it allows expansive exceptions for “national security” and vaguely defined “legitimate interests,” and it envisions a government-controlled Data Protection Authority. Critics warn that without narrowing these loopholes, the new law will fail to meet

international standards or prevent surveillance abuses. As of early 2025 the bill awaits parliamentary debate. (Ali, et al, 2024)

Finally, Pakistan has experienced multiple high-profile data breaches (e.g. of NADRA, tax, and intelligence databases), which have raised public alarm about data security. Experts cite these leaks as evidence of “security gaps” that make state-held personal data vulnerable. These incidents have bolstered calls (including by Justice Sattar) for stronger privacy safeguards and emergency legislation like a data protection act.

European Union:

In Europe, 2023–2025 has brought its own developments. The EU and Council of Europe continue to refine privacy rules. At the supranational level, the Human Rights Council’s October 2023 resolution (A/HRC/54/21) – noted above – was quickly endorsed by the UN General Assembly, signaling broader consensus on banning invasive surveillance tech. Within the EU, policymakers have taken steps addressing surveillance and encryption. In June 2025 the European Commission published a *roadmap* for “lawful and effective access to data by law enforcement”. The plan includes preparing new EU-wide data retention rules (with an impact assessment due by 2025) and measures for cross-border interception. Importantly, the Commission openly acknowledges that any new retention law must comply with past CJEU judgments: data retention must be “strictly necessary” and cannot target “all means of electronic communication” indiscriminately. The roadmap also forms a working group on encryption, aiming to equip police with decryption tools rather than banning strong encryption outright. Thus, even as Europe seeks more tools to fight crime, it reiterates that surveillance must respect human rights.

Another EU highlight is the progress on AI regulation. In 2023 the European Parliament and Council provisionally agreed on the AI Act, which (among other things) will ban law enforcement use of live facial recognition in public spaces and impose strict controls on biometric surveillance (in line with UN recommendations). The AI Act will oblige all high-risk AI systems – including those used for predicting behavior or risks – to adhere to strict transparency, fairness, and oversight standards. (Hacker, P. 2023)

Across Europe, courts continue to police privacy. In 2023 the Court of Justice clarified (in the *La Quadrature du Net* case) that individuals can challenge data-protection authorities for failure to act against unlawful transfers to the US. Meanwhile, national courts have upheld strong search-warrant requirements: for example, the German Constitutional Court held that a suspicion-based search of digital devices without prior judicial approval was unconstitutional (2022).

Global / Tech trends:

More broadly, surveillance is evolving through new technologies: governments worldwide are experimenting with AI-driven predictive policing, social media monitoring, and massive biometrics databases. International bodies (UNICEF, UNESCO, etc.) have started studying the impacts of such tools on child rights and freedom of opinion. However, most proposals (including a pending UN biometric code) are still in discussion and not yet reflected in law.

Taken together, recent developments show that both Pakistan and Europe are grappling with the privacy-vs-security trade-off. Pakistan's case demonstrates how rapid deployment of surveillance tech can outpace legal safeguards, creating public backlash and judicial intervention. The EU shows the opposite spectrum: strong legal frameworks are in place, but they are strained by demands for new security measures (leading to policy reforms and court scrutiny). The coming years (2025–2026) will test whether these jurisdictions can update their laws in a way that both protects citizens and addresses legitimate security needs.

Key Challenges and Gaps in Enforcement

Despite robust legal norms on paper, significant challenges hinder effective privacy protection in Pakistan and elsewhere.

In Pakistan these include:

Lack of Transparency and Oversight.

Intelligence and police agencies operate largely in secret. Even where warrants are required by law (Fair Trial Act 2013), records of actual wiretaps are often classified, and courts have no routine mechanism to review their use. The 2024 LIMS case illustrated that interventions can occur without public knowledge: telecom operators only learned of LIMS when the court order disclosed it. Civil society and journalists have no independent oversight body to appeal to; instead they must file ad hoc lawsuits. The Telecom Authority itself admits it does not reveal which agencies can use its systems. Nighat Dad sharply criticized both the government and telecom companies for failing to inform citizens, observing that telcos could be sued for violating privacy under Article 14. In short, the chain of authorization – from executive order to judicial warrant to telco compliance – is opaque. This gap allows potential abuse (or even unauthorized surveillance) to go unchecked.

Outdated or Overbroad Laws.

Many Pakistani statutes were drafted before digital tech matured. The Telegraph Act and PTA Act, while amended, contain broad “public safety” exceptions. PECA 2016 was passed urgently after terrorism but contained sweeping powers coupled with vague terms (e.g. “glory of Islam,” “morality,” “national security” in blocking orders). In practice, these can be used to censor websites or intercept communications for reasons unrelated to serious crime. Meanwhile, laws like the Monitoring Regulations effectively required all ISPs to build intercept capabilities, despite weak justification in 2010 for society-wide surveillance. The gap between colonial-era statutes and modern technology creates ambiguity: security agencies may claim powers not contemplated by older law. For instance, until 2024 it was unclear whether agencies had formal “authorization” under any law to use LIMS.

No Dedicated Data Protection Regime.

Pakistan's absence of an independent privacy regulator or data-protection law means that even legitimate surveillance activities lack safeguards like data minimization, deletion schedules, or remedies for individuals. The only sectoral privacy rule is that ISPs retain data as a license condition; but enforcement is lax. Citizens whose data is

collected (innocent bystanders) have no clear right to challenge or correct it. Activists warn that the impending Personal Data Protection Bill is weaker than EU norms. Without strong personal data rights enshrined in law, citizens remain vulnerable to incidental or targeted data exploitation by state or private actors.

Weak Judicial Implementation.

Even though Pakistani courts have ruled strongly in favor of privacy, enforcement is spotty. For example, the Fair Trial Act (2013) requires High Court warrants, but it remains routine for investigators to seek communications data informally through police channels. In one Islamabad case, the police admitted that rather than obtaining a judicial warrant, they simply used Section 94 of the Criminal Procedure Code to demand subscriber information from ISPs – a procedure meant for existing records, not live surveillance. The High Court criticized this as a “stretch” of the law. In general, there is little active monitoring to ensure law enforcement follows the formal warrant process; complaints must be litigated ex post.

Political and Security Pressures.

Pakistan’s security environment – ongoing counter-terror operations and political instability – exerts pressure for aggressive surveillance. The Army Public School massacre (2014) and repeated terror incidents have been cited by officials as justification for expansive intercept powers. Intelligence agencies enjoy considerable autonomy, and during emergency rule or military dominance, constitutional rights have often been suspended or ignored. Thus, even if legal standards exist, the political will to enforce them against powerful security agencies may be lacking.

In the EU and Internationally

Although the EU has a robust legal framework, it too faces enforcement gaps and tensions:

Balancing Security vs Rights

European countries grapple with terrorist threats and crime, leading to proposals (like the 2025 roadmap) to expand access to data and limit encryption. Critics fear these measures could erode the hard-won privacy safeguards. Ensuring that any new laws truly meet the CJEU’s “strictly necessary” test is challenging. Civil society pressures lawmakers to apply existing rules (e.g. via infringement actions against member states violating ECtHR case law) rather than legislate new broad powers. The dynamic is similar to Pakistan’s: even democracies find it hard to resist security arguments when drafting surveillance laws.

International Jurisdiction Issues

Surveillance often crosses borders (e.g. telecom routing, cloud storage). No global treaty coordinates oversight. States may request data from foreign providers (through mutual legal assistance) but processes are cumbersome and often fail to protect privacy consistently. For example, after the US invalidated the EU–US Privacy Shield, data transfers became legally fraught. While Pakistan is not in GDPR’s jurisdiction, any foreign tech company operating in Pakistan must still comply with

their home-country privacy rules (as Meta or Google illustrate). This extraterritorial landscape complicates enforcement: even if Pakistan enacts a strong privacy law, enforcing it against foreign companies or states is non-trivial.

Technological Change

Both Pakistan and Europe struggle to keep laws aligned with evolving tech. AI and big data analytics can bypass traditional legal categories. For instance, passive metadata analysis (location tracking) can be as revealing as content. Lawmakers must catch up, but legislative processes are slow. As the UN Special Rapporteur warned, “lack of clarity” on how to apply existing law to global digital networks has undermined rights. In Pakistan, this means laws drafted for telephone taps now must be interpreted in the age of smartphones and internet. Similarly, EU laws struggle with end-to-end encryption – Europe so far avoids mandating “backdoors,” but new pressure groups demand mechanisms for lawful access to encrypted communications.

Enforcement Resource Constraints

Investigating and prosecuting illegal surveillance requires capacity that many countries lack. Even when laws permit oversight, the agencies (judicial or parliamentary) that should audit surveillance may be underfunded or dominated by security interests. Pakistan’s Federal Ombudsman or privacy NGOs have limited power. In Europe, data protection authorities (DPAs) are better resourced, but they typically focus on private-sector data and only secondarily on law enforcement’s access to data.

In summary, key gaps in enforcement include lack of transparency (which breeds suspicion of abuse), outdated or too-flexible laws, insufficient independent oversight, and the challenge of fast-moving technology. Pakistan’s situation is severe – the state’s hand in surveillance is heavy and private recourse is weak – while the EU’s framework is stronger but under strain from new security demands. Both contexts show that robust legal rights to privacy mean little without diligent implementation, judicial scrutiny, and public accountability.

Recommendations for Reform

Addressing these challenges requires action on multiple fronts. For Pakistan, practical reforms should include:

Enact a Robust Data Protection Law with Oversight

Pakistan’s draft Personal Data Protection Bill should be revised in an open, inclusive process to align with global best practices. Ambiguous exemptions (e.g. “national security,” “legitimate interest”) must be narrowed or removed, and there should be a truly independent Data Protection Authority (DPA) empowered to enforce individuals’ rights. The law should guarantee rights of access, correction, and deletion of personal data, and impose strong penalties for violations. Learning from the EU’s GDPR, Pakistan can require that data retention by companies is limited and that metadata collection by law enforcement requires strict justification. Privacy International has warned that the current draft is too weak and risks being “misused

for unlawful surveillance”; Pakistan should heed these concerns by strengthening the bill’s privacy safeguards and providing for judicial review.

Strengthen Judicial Control and Transparency

Implement the Supreme Court’s holding in *Benazir* and the Islamabad High Court’s 2024 order by ensuring that **all** intercepts require prior judicial authorization, as per the *Investigation for Fair Trial Act*. The Fair Trial Act should be strictly enforced, with investigating agencies legally obliged to seek High Court warrants for any wiretap or live surveillance. Any use of LIMS or similar systems without such warrants must be prohibited outright, as ordered by the IHC. Pakistan could also establish a standing court commission or oversight committee (as envisioned in *Benazir*) to audit interception requests and logs. In addition, the government should lift secrecy around surveillance practices: for example, require telecoms to publish transparency reports on compliance with legal orders, and require periodic public reporting (perhaps to Parliament or a parliamentary committee) on the volume and scope of government surveillance activities.

Allow End-to-End Encryption

The 2010 telecom monitoring regulations effectively banned strong encryption by default. Pakistan should reverse this approach. Encryption is a legitimate privacy tool, and lawful intercept can be achieved through lawful warrants without legislating against ciphers. At most, Pakistan might require that providers give required metadata without undermining content encryption. Internationally, bans on encryption are widely seen as weakening security (since they can make systems more vulnerable). Therefore, the government should update its tech laws to allow encrypted services by default and remove any blanket prohibition. If necessary, procedures could be put in place for exceptional cases where courts might require an entity to assist decryption (subject to due process), but not strip the population of encryption wholesale.

Judicial and Legislative Reform:

Courts in Pakistan should more vigorously enforce privacy norms. For instance, judges should entertain privacy challenges and not dismiss them on procedural grounds. The Supreme Court should reaffirm and perhaps expand its earlier privacy rulings, potentially developing a fuller test for surveillance that incorporates necessity and proportionality. Parliament should clarify any remaining ambiguities: e.g. amend the PTA Act to explicitly forbid interception without warrant, repeal obsolete provisions from the colonial Telegraph Act, and set firm penalties for officials who order or conduct unauthorized surveillance. Pakistan could also consider joining or drawing lessons from the Council of Europe Convention 108+ (on data protection), signaling commitment to international privacy standards.

Public Accountability and Remedy

Individuals must have recourse if their privacy is violated. Pakistan should enable litigation or complaints procedures: if an agency eavesdrops illegally, the victim (or affected third parties) should be able to sue for damages or injunctive relief. As Nighat Dad noted, citizens can theoretically take telecoms to court for privacy breaches; in practice, this rarely happens. Legal aid and awareness programs are needed so people know their rights under Article 14. Civil society organizations

should be empowered to petition courts on behalf of victims and to serve as watchdogs. Creating a specialized data protection commission or ombudsman with complaint-handling authority would also provide an avenue for enforcement.

International Cooperation and Advocacy

Pakistan should live up to its international commitments by inviting UN experts (e.g. the Special Rapporteur) to review its laws, and by participating actively in UN initiatives on digital rights. Adopting recommendations from HRC Res. 54/21 – such as prohibiting indiscriminate facial recognition surveillance – could guide national policy. Pakistan might also collaborate with like-minded countries to push for global norms (e.g. at the UN or Commonwealth) that balance tech innovation with human rights.

From a broader perspective, international law itself might evolve to offer stronger protection. The UN Special Rapporteur has called for “best practices” to bring surveillance under the rule of law; Pakistan and others should engage with such guidance. The potential of a new global treaty on digital privacy (perhaps within the framework of human rights or cyber-security conventions) could be explored. In the meantime, drawing on the EU example, Pakistan might negotiate bilateral data-sharing agreements with built-in privacy safeguards, and ensure any overseas surveillance (e.g. through foreign assist) is subject to similar checks.

In summary, reform should **prioritize aligning law with constitutional guarantees**. This means closing loopholes, enforcing judicial oversight, and establishing independent authorities, rather than merely expanding executive power. The experience of other countries suggests that when surveillance is subject to genuine checks and balances, it can be targeted effectively without sweeping violations of privacy. As the Islamabad High Court observed, unauthorised monitoring causes “irreparable harm to the liberty, dignity and privacy of the citizens”. Any reforms must minimize such harm, in line with Pakistan’s obligations under international law and its own constitution.

Conclusion

The 21st century has ushered in unprecedented surveillance capabilities that outstrip older legal frameworks. International law – through the UDHR, ICCPR, regional instruments, and UN resolutions – clearly affirms that privacy is a fundamental right, offline and online. This legal duty is echoed in Pakistan’s Constitution (Article 14) and in emerging global consensus (e.g. bans on remote biometric ID). Yet, law without enforcement cannot protect privacy. Pakistan’s recent experiences, from clandestine mass interception (LIMS) to debates over data-protection laws, illustrate the perils of leaving privacy unprotected. As one legal study noted, Pakistan’s constitution *recognises* privacy as fundamental, even as agencies “conduct heavy surveillance” justified by security concerns. This tension – between rights and security – also plays out in Europe, where strong legal protections are tested by proposals to expand surveillance powers.

If privacy is to survive in the digital age, the letter of international law must be matched by its spirit. Pakistan should implement the guarantees it has solemnly accepted, and it can learn from jurisdictions like the EU in designing oversight

mechanisms. Conversely, democracies should not be complacent: courts in Europe and beyond continue to adjudicate what's necessary and proportionate. The future of privacy protection will depend on this ongoing dialogue between technology, law, and human rights. The international community must help close enforcement gaps – through peer accountability and possibly new treaties – so that no one's communications are swept up without justification.

Ultimately, “privacy in peril” is not an inevitability but a warning. Protecting privacy under international law will require vigilance, innovation, and a recommitment to the principle that, as the UN has asserted, no one should face arbitrary or unlawful interference in their private life. Pakistan's journey, alongside global trends, shows that while threats are growing, so too are the tools of legal protection. With concerted effort, the chilling effect of mass surveillance on freedom can be curtailed, preserving individual dignity and democratic values for the digital era.

References

- Benazir Bhutto v. President of Pakistan, PLD 1998 Supreme Court 388 (Pak.).
- European Data Protection Supervisor. (n.d.). *Charter of Fundamental Rights*. Retrieved February 1, 2025, from https://edps.europa.eu/data-protection/our-work/subjects/charter-fundamental-rights_en.
- González Vidal, S., & Mildebrath, H. A. (2025). *Mapping CJEU limits on data retention frameworks* (EPRS Briefing). European Parliamentary Research Service.
- Human Rights Council (UN). (2023). *A/HRC/RES/54/21 – Right to privacy in the digital age*.
- Human Rights Watch. (2015, July 8). *Bold step on privacy and digital rights*. Human Rights Watch.
- Iqbal, S. (2023, June 20). *The legal landscape for privacy and surveillance in Pakistan*. Global Insight, International Bar Association.
- Khurram, Z. (2024, July 2). *The surveillance system keeping tabs on millions*. Dawn.
- Maynard, P. (2025, June 27). European Commission publishes its plan to enable more effective law enforcement access to data. *InsidePrivacy*. Retrieved from <https://insideprivacy.com/data-privacy/eu-law-enforcement-data-access>.
- Sattar, Justice B. (2024). *Islamabad High Court orders* (oral judgment, July 2, 2024).
- Asad, M. (2024, July 2). *Telecom operators allowed to share suspects' data with police*. Dawn.
- Privacy International. (2023, August 8). *Privacy International raises concerns regarding Pakistan's Personal Data Protection Bill*.
- Privacy International & Digital Rights Foundation. (2019, January). *State of Privacy: Pakistan*.
- United Nations. (1948). *Universal Declaration of Human Rights*, art. 12.
- Générale Colombie. (1997). *Mohtarma Benazir Bhutto v. President of Pakistan*, PLD 1998 SC 388 (Pak.).
- Pakistan. (1973). *Constitution of the Islamic Republic of Pakistan*. (Art. 14).
- Pakistan. (2013). *Investigation for Fair Trial Act, 2013* (Act No. X of 2013).
- Pakistan. (2016). *Prevention of Electronic Crimes Act, 2016* (Act No. XII of 2016).
- Pakistan. (2010). *Monitoring and Reconciliation of Telephony Traffic Regulations*, 2010.

- Pakistan Telecommunications Authority. (2010). *Telecommunications (Re-organization) Act*, 1996, §54.
- Dror-Shpoliansky, D., & Shany, Y. (2021). It's the end of the (Offline) World as we know it: From Human rights to Digital Human rights—a proposed typology. *European Journal of International Law*, 32(4), 1249-1282.
- Ionita, C. V., & Kanetake, M. (2023). International human rights law in the digital age: perspectives from the UN human rights system. In *Research Handbook on Law and Technology* (pp. 235-253). Edward Elgar Publishing.
- Zaki abbas (2024). <https://www.dawn.com/news/1843299#:~:text=%E2%80%A2%20PTA,reaching%20implications>
- Shaelou, S. L., & Razmetaeva, Y. (2023, December). Challenges to Fundamental Human Rights in the age of Artificial Intelligence Systems: shaping the digital legal order while upholding Rule of Law principles and European values. In *ERA Forum* (Vol. 24, No. 4, pp. 567-587). Berlin/Heidelberg: Springer Berlin Heidelberg.
- P L D 1998 Supreme Court 388
<https://www.hrw.org/news/2015/07/08/bold-step-privacy-and-digital-rights#:~:text=But%20while%20advancement%20in%20digital,collection%20of%20their%20personal%20data>
- Psychogiopoulou, E. (2024). Fundamental Rights in CJEU Data Retention Case Law: A Refined Regime in Response to Member States' Concerns, or Compensating for the Lack of Legislative Intervention in the Digital Age?. *J. Intell. Prop. Info. Tech. & Elec. Com. L.*, 15, 194.
- Sahar Iqbal <https://www.ibanet.org/legal-landscape-for-privacy-surveillance-in-Pakistan#:~:text=Pakistan%20is%20a%20signatory%20to,includes%20provisions%20in%20Article%2018>
- Eeckhout, P. (2002). The EU Charter of Fundamental Rights and the federal question. *Common Market Law Review*, 39(5).
- Custers, B. (2022). New digital rights: Imagining additional fundamental rights for the digital era. *Computer Law & Security Review*, 44, 105636.
- UN General Assembly 2023, Resolution 54/21 on the Right to privacy in the digital age
- Psychogiopoulou, E. (2024). Fundamental Rights in CJEU Data Retention Case Law: A Refined Regime in Response to Member States' Concerns, or Compensating for the Lack of Legislative Intervention in the Digital Age?. *J. Intell. Prop. Info. Tech. & Elec. Com. L.*, 15, 194.
- Constitution of Islamic Republic of Pakistan, 1973.
- PECA Acti 2016.
- Malik Asad (2024), <https://www.dawn.com/news/1843310/telecom-operators-allowed-to-share-suspects-data-with-police#:~:text=As%20per%20the%20court%20order%2C,being%20surveilled%2C%E2%80%9D%20Justice%20Sattar%20ruled>
- Kellerbauer, M., Klamert, M., & Tomkin, J. (2024). *The EU Treaties and Charter of Fundamental Rights: a Commentary*. Oxford University Press.
- Lubin, A. (2022). *Big Brother Watch v. UK* (Eur. Ct. HR Grand Chamber).

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

International Legal Materials, 61(4), 605-653.

Paul Mayrand (2025), <https://www.insideprivacy.com/data-privacy/european-commission-publishes-its-plan-to-enable-more-effective-law-enforcement-access-to-data/#:~:text=On%2024%20June%202025%2C%20the,Data%20for%20Effective%20Law%20Enforcement>

Ebers, M. (2023). The European Commission's Proposal for an Artificial Intelligence Act. In Research Handbook on EU Internet Law (pp. 271-292). Edward Elgar Publishing.

Kemal, A. A., & Shah, M. H. (2024). Digital innovation in social cash organizations—the effects of the institutional interactions for transforming organizational practices. *Information Technology & People*, 37(5), 2092-2126.

Ali, M. I., & Hussain, K. A. (2024). Unveiling the tapestry: a comparative investigation into data-protection legislation in India and Pakistan. *Socrates Rīga Stradiņš Univ Fac Law Electron Sci J Law*, 1, 1-8.

Hacker, P. (2023). AI regulation in Europe: from the AI act to future regulatory challenges. *arXiv preprint arXiv:2310.04072*.