Saving Privacy Rights: ICT Companies, Government Surveillance, and the Battle for Privacy in Pakistan

Philip Paik, GW Law Civil and Human Rights Law Clinic

September 2025

Table of Contents

I. Introduction

In the battle to protect privacy rights, Information and Communication Technology (ICT) companies operating in Pakistan often find themselves in a bind—caught between the demands of an authoritarian state and their duty to uphold human rights. Since 2022, a political barrage has been rattling Pakistan with a series of high-profile audio leaks that surfaced online involving senior government officials and opposition leaders. The leaks, widely suspected to have originated from government intelligence agencies, exposed private conversations and sensitive political strategies between political figures. The fallout was immediate and severe—public trust in the government was further undermined, opposition parties decried the surveillance as unconstitutional, and civil society groups raised alarms about the growing encroachment on privacy. The scandal underscored a longstanding and deeply troubling reality in the country: the prevalent use of highly intrusive surveillance technologies with little to no accountability.[1]

This situation raises a critical question: what are the responsibilities of ICT companies operating in regimes like Pakistan, when confronted by potentially unlawful government demands to deploy highly intrusive surveillance technologies against the public and political figures?[2] As conduits for the transmission of data and telecommunications, ICT companies are often beset by governments' demands to engage in surveillance. When such governments demand access to user data or pressure companies to otherwise invade the privacy of public and political figures, ICT companies face complex legal, ethical, and operational challenges. The situation in Pakistan thus reflects a broader global issue: how should private companies balance their legal obligations to host governments with their responsibility to protect user data and personal privacy—an internationally recognized human right?

[1] Faaiza Qazi, *The Politics of Exposure: Audio Leaks and the Erosion of Privacy and Democracy in Pakistan*, Digital Privacy Rights Resource 1, 15 (July 2025).
[2] The Economist Intelligence Unit, *Democracy Index 2023*, at 15 (2024) (noting that Pakistan dropped 11 places in the index and was reclassified as an authoritarian regime).

This Article argues that ICT companies should adhere to international standards that recognize their responsibility to respect human rights, including privacy, as outlined in the United Nations Guiding Principles on Business and Human Rights (UNGPs) and by the Global Network Initiative (GNI), a multi-stakeholder initiative that implements the UNGPs for the ICT sector.[3][4] The UNGPs, endorsed by the UN Human Rights Council in 2011, provide a global framework for businesses to prevent and address human rights impacts, emphasizing accountability and due diligence.[5] When operating in countries that actively suppress digital rights, such as Pakistan, this responsibility becomes even more urgent and morally significant. ICT companies are not merely passive players; they are intermediaries with the capacity to shape the frontiers of digital rights and privacy protections.

To illustrate the context in which these issues arise, this Article will first briefly discuss the Audio Leaks Cases in Pakistan, examining how abusive State surveillance practices jeopardize privacy rights that implicate corporate responsibility. It will then outline the principles of international law governing the responsibility of ICT companies to respect human rights, focusing on privacy and data protection standards. Finally, it will analyse the pathways available to ICT companies when confronted with arbitrary surveillance demands from repressive regimes, highlighting strategies that align with international human rights norms while addressing local legal constraints.

A. What the Audio Leaks Cases Tells Us About ICT Company Compliance Challenges[6]

The Audio Leaks Cases (ALC) in Pakistan underscores the challenges that ICT companies face when navigating the complex and often contradictory terrain of corporate compliance with human rights in repressive regimes. This case study reveals the precarious position of companies that must balance compliance with domestic legal requirements against their responsibility to uphold international privacy standards. The ALC scandal involved unauthorized releases of private conversations among senior government officials and political opposition figures, suggesting that high-level surveillance operations were being conducted without transparency or proper legal oversight. This inference highlights how difficult it is for ICT companies to protect privacy rights when government demands for user data or surveillance are politically motivated. The ALC also demonstrates how domestic privacy regulations in Pakistan are fluid and unpredictable, with judicial decisions and legislative amendments often shifting the compliance landscape overnight. The challenge for ICT companies lies in navigating this legal instability while attempting to uphold international privacy norms and avoid punitive measures from the state.

This part examines how the ALC exposed three interrelated compliance challenges for ICT companies: 1) rapidly changing domestic privacy protections and surveillance powers; 2)

---

[3] United Nations, *Guiding Principles on Business and Human Rights*, U.N. Doc. A/HRC/17/31 (Mar. 21, 2011), https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf (last visited Mar. 25, 2025) [hereinafter UNGPs].

[4] Global Network Initiative Principles, Global Network Initiative, https://globalnetworkinitiative.org/gni-principles/ [https://perma.cc/GHI3-JKL4] (last visited Mar. 25, 2025).

[5] UNGPs, *supra* note 3.

[6] Qazi, *supra* note 1, at 13-15.

legal uncertainty stemming from political instability; and 3) the resulting dilemma for companies between respecting international privacy norms and complying with arbitrary domestic demands and/or norms.

1. Rapidly changing privacy and surveillance laws

One of the key challenges highlighted by the Audio Leaks case is the volatility of Pakistan's legal framework on privacy and surveillance. The 2013 Investigation for Fair Trial Act (IFTA) is the primary legislation governing electronic surveillance in Pakistan.[7] Additionally, Section 54 of the 1996 Pakistan Telecommunication (Re-Organization) Act (PTRA)—which establishes the Pakistan Telecommunication Authority (PTA)—vests the federal government with broad and disruptive powers of surveillance in the name of national security, specifically the ability to trace calls or suspend licenses during a war or period of hostilities by a foreign power against Pakistan, or upon a proclamation of emergency by the president.[8] This instability forces ICT companies to frequently revise their compliance strategies, increasing both legal costs and operational uncertainty.

2. Legal uncertainty and political instability

Pakistan's volatile political climate further complicates compliance efforts. Surveillance tools and the data they produce have become powerful political weapons. The ALC illustrated how state surveillance is heavily politicized, with the current government exerting significant pressure on companies to comply or face immediate retaliation. Companies face intense pressure to meet intrusive surveillance demands to avoid fines, license revocations, or other regulatory penalties imposed by the existing regime, as non-compliance risks swift and severe punitive action. Companies also face pressure to comply with intrusive surveillance demands to avoid fines, license revocations, or other regulatory penalties. This creates a climate of uncertainty where companies must prioritize short-term compliance to mitigate the current government's threats, even as they navigate the long-term reputational and legal consequences of such actions.[9]

3. The dilemma of conflicting privacy standards

Conflicts between domestic and international privacy standards place ICT companies in a difficult position. International frameworks based on the International Covenant on Civil and Political Rights (ICCPR), like the UNGPs, establish an obligation for companies to respect the

[7] *Id*.
[8] *Id.* at 6-7.
[9] BSR/JustPeace Labs, Toolkit & Primer on Tech Sector eHRDD in CAHRA [2022] ("BSR/JustPeace Labs Toolkit on eHRDD"), https://justpeacelabs.org/wp-content/uploads/2022/11/JPL-BSR-eHRDD-Toolkit-Primer.pdf (Primer), https://justpeacelabs.org/wp-content/uploads/2022/11/JPL-BSR-Conflict-Sensitive-HRDD-for-Tech.pdf (Toolkit) (last visited Mar. 30, 2025) (discussing the challenges tech companies face in balancing compliance with surveillance demands against long-term political and legal risks in conflict-affected areas).

right to privacy.[10] Unlike the ICCPR, which legally binds states to respect and protect individuals' right to privacy, the UNGPs outline both states' duty to protect against business-related human rights abuses and companies' responsibility to respect rights, like privacy, through due diligence.[11] The Global Network Initiative Principles provide voluntary guidance specifically for member tech companies to uphold human rights.[12]

However, these standards may seem unrealistic or unachievable to ICT companies operating in countries with authoritarian regimes, where domestic privacy regulations can be unclear, shifting, or ignored at best, and at worst, patently repressive. Companies face a strategic dilemma when complying with authoritarian surveillance demands that are arbitrary or abusive, risking criticism or reputational harm from international human rights advocates, though this backlash often lacks significant impact. Resistance or partial defiance typically triggers immediate domestic pressure, including operational restrictions, public accusations, or market exclusion, beyond just fines or license revocations.[13]

The Audio Leaks Case illustrates how ICT companies operating in repressive regimes can be pressured by state authorities to engage in conduct contrary to the relevant standards emanating from the UNGP framework. How should they respond? That is the subject of the next Part. The legal and political instability surrounding privacy rights in Pakistan creates a high-risk environment where compliance decisions carry both immediate and long-term political and reputational risks. Caught between volatile legal frameworks, politicized surveillance demands, and divergent privacy expectations, companies must navigate a minefield where every decision carries significant moral, ethical, and even potentially legal consequences. Fortunately, they have guidance they can draw upon to do so.

II. ICT Companies' Responsibility to Respect Human Rights

This section examines the international legal normative framework governing the responsibility of ICT companies to respect human rights, with a particular focus on the right to privacy. The framework is primarily guided by the UNGPs and the GNI Principles.[14] As noted already, GNI is an international forum where company and civil society representatives convene to promote freedom of expression and privacy rights online. As noted above, the UNGPs establish a global standard for businesses to prevent and mitigate human rights impacts through due diligence and accountability measures.[15] The GNI Principles commit ICT companies to uphold freedom of expression and privacy rights, while

[10] International Covenant on Civil and Political Rights (ICCPR), Dec. 16, 1966, 21 U.S.T. 521; 999 U.N.T.S. 171.
[11] ICCPR, *supra* note 9, art. 17(1); UNGP on Business and Human Rights, *supra* note 3, princ. 1.
[12] GNI Principles, *supra* note 4.
[13] ARTICLE 19, *Engaging tech for internet freedom in authoritarian countries* (2024), https://www.article19.org/engaging-tech-for-internet-freedom/.
[14] UNGPs, *supra* note 3; GNI Principles, *supra* note 4.
[15] UNGPs, *supra* note 3.

the Implementation Guidelines offer practical measures for conducting human rights due diligence and addressing government requests for data or censorship.[16]

A. Under the UNGPs, ICT companies have a responsibility to respect the right to privacy as a human right.

1. ICT companies should enact policies to avoid infringing on the privacy rights of others, recognizing that the right to privacy is an internationally recognized human right.

Under the UNGPs, ICT companies are called upon to respect the right to privacy as a fundamental human right.[17] Principle 11 of the UNGPs states that companies should first adopt policies and practices to ensure they do not infringe on the privacy rights of others.[18] The right to privacy is an internationally recognized human right that companies should respect globally, regardless of state actions or national laws. Companies are expected to take proactive steps to prevent, mitigate, and remedy any harms to privacy rights.[19] This includes enacting human rights policies and effectively implementing them in their business operations. Furthermore, companies should avoid undermining state human rights obligations or judicial integrity when addressing privacy concerns.[20]

Under Principle 12 of the UNGPs, ICT companies are expected to respect the right to privacy as a recognized human right.[21] Companies should give heightened attention to individuals and groups most at risk of privacy violations in specific industries or contexts. Vulnerable groups, including journalists, women, religious minorities, and political opponents, warrant particular consideration.[22]

The GNI Principles reinforce these obligations and apply them specifically to ICT companies that agree to adhere to them.[23] According to the GNI Principles' Preamble, ICT companies joining GNI should respect and promote both freedom of expression and privacy rights as expressed therein.[24] Companies in GNI are expected to support privacy rights through responsible business decisions, shared learning, and collaboration with other stakeholders.[25] While these companies are required to comply with local laws, they must also strive to uphold international human rights standards and minimize any adverse impacts arising from

---

[16] Global Network Initiative, *GNI Principles and Implementation Guidelines*, https://globalnetworkinitiative.org/gni-principles/; https://globalnetworkinitiative.org/implementation-guidelines/.
[17] UNGPs, *supra* note 3, princ. 11.
[18] *Id*.
[19] *Id*.
[20] *Id*.
[21] *Id*.
[22] *Id*.
[23] GNI Principles, s*upra* note 4, preamble.
[24] *Id*.
[25] Global Network Initiative, *Members*, https://globalnetworkinitiative.org/who-we-are/members/ (key members include Google, Meta, Microsoft, Nokia, Orange, Telenor Group, Verizon, Vodafone Group, Ericsson, Telia Company, Yahoo).

conflicting national legal frameworks.[26] Although the GNI Principles apply only to those ICT companies that are members of GNI, they provide expert normative guidance for the ICT sector as a whole on how the UNGP should apply to such companies.[27]

GNI Principle 3 defines privacy as a fundamental human right that protects human dignity, security, and freedom of expression.[28] All individuals have the right to legal protection against unlawful or arbitrary interference with their privacy. Accordingly, under the GNI Principles framework, ICT companies are responsible for safeguarding user privacy on a global scale, even when faced with intrusive government demands. Companies are expected to uphold international standards and resist pressures that conflict with these fundamental privacy protections.

2. ICT companies should conduct thorough due diligence and risk assessments to identify, prevent, mitigate, and address potential privacy rights violations arising from their business activities.

Under Principle 13 of the UNGP on Business and Human Rights, businesses must avoid causing or contributing to human rights harms and take action to address them when they occur.[29] Even if a company is not directly responsible for a violation, it must still prevent or mitigate human rights harms linked to its operations, products, or services through business relationships.

The GNI Principles reinforce this obligation by requiring ICT companies to identify situations where privacy rights may be jeopardized or advanced and to integrate these findings into their decision-making processes.[30] Section 3.4 of the GNI Implementation Guidelines specifically states that participating companies must assess the human rights risks associated with the collection, storage, and retention of personal information in the jurisdictions where they operate.[31] This means companies need to evaluate how their data practices, including cross-border data transfers and government surveillance requests, could affect users' privacy rights.

Principle 17 of the UNGPs further establishes that human rights due diligence should involve an ongoing process of assessing actual and potential privacy rights impacts, acting upon the findings, tracking responses, and communicating how these impacts are being addressed.[32] Due diligence should not be a one-time exercise; it must adapt and conform to evolving risks

[26] *Id*.
[27] GNI Principles, s*upra* note 4; United Nations, B-Tech Project, OHCHR and Business and Human Rights, https://www.ohchr.org/en/business-and-human-rights/b-tech-project (last visited Mar. 30, 2025) (offering guidance on applying the UNGPs to technology companies, reinforcing sector-wide human rights standards).
[28] GNI Principles, *supra* note 4, princ. 3.
[29] UNGPs, *supra* note 3, princ. 13.
[30] GNI Principles, s*upra* note 4, princ. 4.
[31] Global Network Initiative, *Implementation Guidelines*, §3.4, https://globalnetworkinitiative.org/implementation-guidelines/https://globalnetworkinitiative.org/implementation-guidelines/ (last visited Mar. 30, 2025) (provided to GNI member companies to clarify their understanding of how the GNI Principles apply in practice and guide their implementation through specific actions).
[32] UNGPs, *supra* note 3, princ. 17.

over time and begin early in the development of new activities or business relationships, including mergers, acquisitions, and contractual agreements.[33] By implementing robust human rights policies and due diligence frameworks, ICT companies can ensure they meet international human rights standards while safeguarding user privacy.

3. ICT companies should be transparent about their human rights impacts, disclosing policies and practices related to government surveillance requests and user data protection.

ICT companies have a responsibility to be transparent about their human rights impacts, especially concerning government surveillance requests and user data protection practices. Under Principle 21 of the UNGPs, companies are expected to communicate externally about how they address human rights impacts, especially when affected stakeholders raise concerns.[34] For companies operating in high-risk contexts, this obligation extends to formally reporting on how they manage human rights risks and impacts. Communication should be provided in a form and frequency that accurately reflects the company's human rights impact and ensures accessibility for the intended audience.[35]

The GNI Principles reinforce these transparency obligations by establishing a framework for governance, accountability, and transparency. According to GNI Principle 6, companies must operate under a collectively determined governance structure that clearly defines roles and responsibilities, ensuring that accountability is maintained.[36] Transparency should include public disclosure of human rights policies and practices as well as independent assessments of the company's implementation efforts.[37] By adopting transparent communication and governance structures, ICT companies can build trust with stakeholders and demonstrate their commitment to respecting privacy rights and broader human rights standards.

B. Obligations of ICT Companies in Responding to Arbitrary Surveillance Requests from Repressive Regimes

Further building on the framework established by the UNGPs as well as the GNI Principles and Implementing Guidelines, this section examines the obligations of ICT companies when responding to arbitrary surveillance requests from authoritarian regimes. It outlines key international standards that ICT companies should adhere to and the practical challenges they face when domestic laws conflict with global privacy norms. The suggested framework guides ICT companies with strategies to balance legal compliance, corporate responsibility, and human rights protection in authoritarian regimes.

[33] *Id*.
[34] UNGPs, *supra* note 3, princ. 21.
[35] *Id*.
[36] GNI Principles, *supra* note 4, princ. 6.
[37] *Id*.

1. ICT companies should encourage governments to establish legal regimes that comply with international standards on human rights, including privacy rights.

ICT companies have a broader responsibility to promote alignment between domestic regulations and international privacy standards. Section 3.1 of the GNI Implementation Guidelines advises companies to encourage governments to adopt specific, transparent, and consistent legal frameworks governing surveillance and privacy.[38] Governments should be urged to harmonize their domestic regulations with international human rights standards, particularly those related to freedom of expression and the right to privacy.[39]

To support this effort, companies should develop internal policies and procedures that guide how they anticipate, assess and respond to government demands for content restrictions or disclosure of personal information.[40] By adopting a structured approach, companies can ensure that their own actions, as well as their responses to government demands, remain consistent with international human rights obligations. Encouraging governments to comply with international standards helps establish a more predictable and rights-respecting legal environment, even in politically restrictive jurisdictions.

2. ICT companies should require the government to follow established domestic legal processes that implement or reflect international human rights standards.

ICT companies should require governments to comply with domestic legal procedures when seeking to access user information or restrict communications. According to Section 3.2 of the GNI Implementation Guidelines, companies should ensure that any government demand for personal data, content removal, or communication restrictions follows established domestic legal processes.[41] The GNI Implementation Guidelines emphasize that companies should request clear written communications from the government explaining the legal basis for such demands.[42] This ensures that the company's response is based on a transparent and well-defined legal framework. Moreover, Section 3.5 of the GNI Implementation Guidelines encourages companies to operate transparently when responding to government requests.[43] Transparency includes informing users about government requests where legally possible and issuing public reports that summarize the nature and scope of such requests. This approach helps prevent governments from overstepping legal boundaries and ensures that companies uphold their commitment to protecting user privacy and freedom of expression.

3. ICT companies should challenge overbroad, arbitrary, or otherwise unlawful government restrictions.

When governments make surveillance requests that exceed legal limits, ICT companies are encouraged to push back. Section 3.3 of the GNI Implementation Guidelines urges companies to seek clarification or modification from authorized officials when surveillance requests

[38] GNI Implementation Guidelines, *supra* note 27, §3.1.
[39] UNGPs, *supra* note 3, princ. 1–10 (Pillar I).
[40] UNGPs, *supra* note 3, Pillar II.
[41] GNI Implementation Guidelines, *supra* note 27, §3.2.
[42] *Id*.
[43] GNI Implementation Guidelines, *supra* note 27, §3.5.

appear overbroad or unlawful.[44] If the government's response remains unsatisfactory, companies should engage with relevant stakeholders, including relevant government authorities, international human rights bodies, and non-governmental organizations, to seek further guidance and support.[45]

In cases where the government's actions would clearly violate domestic legal standards, companies are encouraged to challenge such measures through domestic courts. Such legal challenges not only protect the rights of individual users but also set important precedents that may influence future government conduct. Taking legal action demonstrates the company's commitment to defending user rights and upholding global privacy norms even in difficult political environments.[46]

4. ICT companies should move to uphold human rights and privacy when domestic laws and/or government conduct conflict with international standards.

ICT companies have a responsibility to uphold human rights and protect user privacy, even when domestic laws and/or government conduct conflict with internationally recognized standards. According to Principle 23(b) of the UNGPs, businesses must respect human rights regardless of the political or legal context in which they operate.[47] When domestic laws prevent full compliance with international human rights standards, companies should strive to honor these international standards and principles to the greatest extent possible and demonstrate their efforts to mitigate harm.[48]

The GNI Principles reinforce the expectation that companies will protect user privacy. ICT companies will respect and work to protect the privacy rights of users when confronted with government demands, laws, or regulations that compromise privacy in a manner inconsistent with internationally recognized laws and standards.[49] Companies should treat human rights risks as legal compliance issues and take steps to reduce potential harm.[50]

ICT companies can take several steps to navigate these complex challenges. They can seek advice from internal cross-functional teams and external experts, including governments, civil society, national human rights institutions, and multi-stakeholder initiatives.[51] Collaboration and consultation with stakeholders can help companies develop more effective strategies for responding to government demands while maintaining a strong commitment to human rights and privacy. Moreover, ICT companies can challenge overbroad, arbitrary, or unlawful requests by demanding formal legal justifications and operating with transparency.[52] They can report the nature and frequency of government requests for user data or surveillance, for example. Upholding these principles helps maintain user trust and ensures that ICT companies remain aligned with international human rights norms.

---

[44] GNI Implementation Guidelines, *supra* note 27, §3.3.
[45] *Id*.
[46] *Id*.
[47] UNGPs, *supra* note 3, princ. 23(b).
[48] *Id*.
[49] GNI Principles, *supra* note 4, princ. 6.
[50] GNI Implementation Guidelines, *supra* note 27, § 2.7(a).
[51] GNI Implementation Guidelines, *supra* note 27, §§ 4.2, 4.4.
[52] GNI Principles, *supra* note 4, princ. 6.

III. Audio Leaks Case Analysis

This section applies the principles derived from international privacy and human rights standards to the challenges identified in the Audio Leaks Cases (ALC), offering a framework for ICT companies operating in Pakistan to navigate surveillance requests by authoritarian regimes. Readers are encouraged to review and refer to the accompanying ALC Article when reading the following sections that offer an analysis of the cases in light of the framework set out in the previous Part. This analysis demonstrates how ICT companies, especially telcos, can take proactive steps to anticipate and mitigate legal and reputational risks in such settings while reinforcing global human rights protections against government overreach.

A. Why Businesses Should Uphold Human Rights in Pakistan

The Audio Leaks Cases in Pakistan highlight the need for ICT companies to prioritize human rights, not only as a moral obligation but also as a strategic necessity for sustainable operations and global trust. As articulated by the United Nations High Commissioner for Human Rights (UNHCR), businesses thrive in environments where human rights are respected, as these conditions foster stability, trust, and economic resilience.[53] In Pakistan, where unauthorized surveillance erodes public confidence, telecommunication companies (telcos) can play a pivotal role in promoting a human rights-based economy. Such an economy ensures fairness, sustainability, and accountability, aligning corporate practices with the public good.[54] These companies make up substantial portions of the Pakistani telecoms market.[55] Their commitment to frameworks like the UNGPs and GNI Principles is essential for addressing privacy challenges and fostering a rights-respecting environment in Pakistan's complex regulatory landscape. By upholding privacy rights, telcos and other ICT companies can mitigate risks of complicity in abuses, which could lead to legal liabilities, reputational damage, and loss of market trust—particularly in jurisdictions with stringent data protection laws.[56]

Moreover, human rights and business interests are interdependent. The UNHCHR emphasizes that businesses need human rights to maintain legitimacy and access to global markets, while human rights rely on businesses to drive accountability and innovation.[57] In

---

[53] Volker Türk, High Comm'r for Human Rights, *Human Rights Economy: Concept & Practical Application*, U.N. Off. High Comm'r for Human Rights (June 11, 2024), https://www.ohchr.org/en/statements-and-speeches/2024/06/human-rights-economy-concept-practical-application.

[54] Ctr. for Econ. & Soc. Rights, *A Rights-Based Economy: Putting People and Planet First* (2023), https://www.cesr.org/sites/default/files/Rights%20Based%20Economy%20briefing.pdf.

[55] Qazi, *supra* note 1, at 20.

[56] Yessica Chong, *Surveillance, Scandals, and Secrets: The Relevance of South Korean Government Surveillance to the Audio Leaks Case in Pakistan*, Collaborative Online Privacy Archive (COPA) (2025). For example, the article discusses how KakaoTalk, a popular South Korean messaging app, revised its data protection policies to enhance encryption and limit government access to user data in response to concerns about state surveillance in South Korea. *See id.*

[57] Volker Türk, High Comm'r for Human Rights, *Business Needs Human Rights and Human Rights Need Business*, U.N. Off. High Comm'r for Human Rights (Dec. 10, 2024),

the context of the Audio Leaks Cases, telcos that resist arbitrary surveillance demands demonstrate leadership in fostering trust and stability, which are essential for long-term profitability. For instance, Telenor Pakistan's affiliation with the GNI positions require it to uphold industry standards by aligning with international norms, enhancing its global reputation. Such affiliation should be emulated by the multinational corporations operating in Pakistan. The OHCHR further notes that in uncertain times, responsible business conduct—rooted in human rights due diligence—helps companies navigate complex political landscapes like Pakistan's, where legal instability and politicized surveillance create operational risks.[58]

Finally, the global community increasingly expects businesses to act as human rights advocates. At the 2024 UN Forum on Business and Human Rights, the High Commissioner urged companies to integrate human rights into their core strategies, recognizing their capacity to influence policy and practice.[59] For ICT companies in Pakistan, this means following the principles highlighted in this Article, to protect users and set precedents for accountability. By doing so, they not only comply with frameworks like the UNGPs on but also contribute to a stable, rights-respecting environment that benefits both society and their bottom line.

1. ICT companies should encourage governments to implement legal regimes that comply with international standards on human rights, including privacy rights.

The recent Audio Leaks Cases in Pakistan sparked serious concerns about unauthorized surveillance, government overreach, and violations of privacy rights, placing telco and other ICT companies at the forefront of a critical effort to safeguard human rights. In response, telcos operating in country should take proactive steps to promote adherence to international privacy and human rights standards, as indicated by the GNI Principles and Implementing Guidelines. They could begin by advocating for specific, transparent, and consistent legal frameworks governing surveillance requests, urging the Pakistani government and the Pakistan Telecommunication Authority (PTA) to align domestic laws with global norms, such as those in the ICCPR and the UNGPs, rather than relying on ambiguous legislation like the 1885 Telegraph Act which permits the State to possess wireless telegraphs upon a vague exclamation of public safety.[60] Additionally, these companies should encourage government policies that reflect international standards on privacy and freedom of expression, working with civil society advocates to support reforms that address the gaps exposed by the PTA's broad claims of authority and the lack of

https://www.ohchr.org/en/statements-and-speeches/2024/12/business-needs-human-rights-and-human-rights-need-business.

[58] Nada Al-Nashif, Deputy High Comm'r for Human Rights, *Responsible Business in Uncertain Times*, U.N. Off. High Comm'r for Human Rights (Oct. 30, 2024), https://www.ohchr.org/en/statements-and-speeches/2024/10/deputy-high-commissioner-responsible-business-uncertain-times.

[59] Volker Türk, High Comm'r for Human Rights, *Forum on Business and Human Rights: World Looks to Business to Play Its Part*, U.N. Off. High Comm'r for Human Rights (Nov. 25, 2024), https://www.ohchr.org/en/statements-and-speeches/2024/11/hc-turk-forum-business-and-human-rights-world-looks-business-play.

[60] Qazi, *supra* note 1, at 10.

warrants in the Audio Leaks Cases. Finally, to ensure their own readiness, ICT firms should establish internal policies and procedures for assessing and responding to government demands regarding unauthorized surveillance or personal data disclosures; they can do this by drawing on Principle 13 of the UNGPs to implement thorough due diligence procedures and mitigate risks associated with tools like the Lawful Intercept Management System (LIMS) and direct intelligence agency access.[61]

2. ICT companies should require the government to follow established domestic legal processes when these implement or reflect international human rights standards.

In light of the ALC controversy, telcos and other ICT companies operating in Pakistan should take extra precautions to ensure that government surveillance requests are legally justified and procedurally sound, particularly when domestic legal processes align with or reflect international human rights standards. Telecommunication companies with important market shares should insist that the government adheres to established procedures, such as those outlined in Pakistan's 2010 Telecommunication (Reorganization) Act, 2016 Fair Trial Act, and Section 54 of the 1996 Telecom Act, ensuring that any interception is authorized by a High Court judge or backed by clear legal provisions. They should also demand clear, written justifications from authorities, specifying the legal basis for surveillance requests, especially given the PTA's assertion of national security authority without warrants. Transparency is crucial; telcos should operate openly by documenting and publicly reporting government-imposed restrictions on privacy and freedom of expression wherever possible, using their market influence to set a precedent. Finally, to counter the risks highlighted by the confirmed use of LIMS and potential direct access by intelligence agencies, these companies could implement strong encryption and data protection measures to minimize unauthorized government interception of communications, thereby protecting user privacy.[62]

3. ICT companies should challenge overbroad, arbitrary, or otherwise unlawful government restrictions.

The ALC starkly demonstrate the dangers of unchecked surveillance powers, as evidenced by the unauthorized recording and dissemination of private conversations involving figures like Bushra Bibi and Mian Najamul Saqib. To counter this overreach, the telcos affected should, to the extent possible, challenge overbroad, arbitrary, or unlawful government restrictions. For example, they could seek clarification or modifications from relevant authorities when faced with vague or overly broad requests, like questioning the PTA's reliance on ambiguous legal authorities like Notification under PTA 926, which authorizes the Inter-Services Intelligence (ISI) without clear legal backing. They could also engage with international human rights organizations and NGOs for support and advocacy, leveraging "best practices" as reflected in the GNI principles to amplify their efforts and push back against politicized

[61] *Id.* at 4.
[62] *Id.*

surveillance.[63] One key lesson from the GNI is that concerted, collective action by companies facing similar challenges is often more effective than individual efforts, enabling telcos operating in a country such as Pakistan to jointly advocate for clearer legal standards and resist unlawful government demands through shared strategies and GNI's multi-stakeholder platform.[64]

Telcos and other ICT companies are understandably constrained in what actions they can take as businesses operating in a difficult environment. Operating in Pakistan's complex regulatory and political landscape, telcos and ICT companies face significant risks when challenging government demands, including potential license revocations, persecution of staff, or targeting of infrastructure, which could severely disrupt operations.[65] These risks must be carefully weighed against their responsibilities under international frameworks like the UNGPs and GNI Principles to protect user privacy and prevent complicity in human rights abuses.

Nonetheless, following the example of Bibi and Saqib's legal challenges, companies could pursue legal action in domestic courts to contest illegitimate government demands, particularly after the Supreme Court's July 2024 directive halting Islamabad High Court proceedings in the ALC investigations.[66] Public disclosure is another vital strategy; although there are real risks involved, Jazz, with its significant market presence, and Zong could under certain circumstances publicly report instances where government requests fail to align with legal standards or international privacy frameworks to hold authorities accountable and protect user rights.

4. Even when governments fail to do so, ICT companies should act to uphold human rights and privacy when domestic laws and/or government conduct conflict with international standards.

Even when the government fails to adhere to international standards, ICT companies should remain committed to upholding these principles, acting to the extent possible as champions of human rights and privacy in the face of conflicting domestic laws and government conduct. For example, they could implement stringent internal compliance measures based on global best practices in privacy and security, ensuring that firms like Telenor adopt policies that mirror the GNI and UNGP guidelines, even when Pakistani laws fall short. Similarly, transparency reports are essential; Telenor, with its GNI affiliation, should lead by example, publicly detailing how it handles PTA demands and any direct access by intelligence agencies, as revealed in the Saqib and Bibi leaks.[67] Strengthening digital security protocols is equally critical, with companies investing in technologies to resist unauthorized LIMS access and prevent breaches like those in November 2023 and other instances.[68]

[63] *Id*.
[64] GNI Principles, *supra* note 4.
[65] Engaging Tech for Internet Freedom in Authoritarian Countries, *supra* note 14.
[66] Qazi, *supra* note 1, at 25-26.
[67] *Id*.
[68] *Id*.

Finally, collaboration is key; multinational corporations should partner not just with each other and other ICT companies in similar situations, but also with international organizations and global civil society to reinforce accountability and advocate for legal reforms, using their international influence to push for a more rights-respecting environment in Pakistan, even when domestic authorities lag behind.

IV. Conclusion

ICT companies operating in authoritarian regimes like Pakistan face significant challenges in balancing legal compliance with their responsibility to uphold human rights, as vividly illustrated by the Audio Leaks Cases. These scandals underscore the risks these firms encounter when governments use surveillance tools for political purposes, making compliance with privacy rights particularly daunting. International frameworks like the UNGPs and the GNI Principles provide clear guidance, asserting that businesses should respect privacy rights regardless of domestic laws and take proactive steps to mitigate human rights violations.

When domestic legal standards conflict with international human rights norms, ICT companies should engage in dialogue with governments to encourage legal reforms that align with global privacy standards, challenge overbroad or unlawful surveillance requests through domestic courts, international human rights bodies, and advocacy groups, and insist on clear legal justifications and written communications outlining the basis for surveillance demands. They can also implement robust internal policies and procedures consistent with international law, seek international legal and diplomatic support to resist restrictive domestic laws, and demonstrate compliance through transparency measures like public reporting on government demands and responses.

Perhaps most significantly, even if the government fails to follow international standards, companies should commit to upholding these principles, leveraging their global influence—if they are multinational corporations—to advocate for stronger privacy protections while minimizing legal and operational risks in authoritarian contexts. It is understood that Telcos in Pakistan face significant risks, such as license revocation and staff persecution, when challenging government demands, but must balance these against their UNGP and GNI obligations to protect user privacy and prevent human rights abuses. On the other hand, a failure to adopt at least some of the strategies discussed in this Article in response to these challenges could result in notable consequences, including legal liability, reputational damage, and regulatory penalties in jurisdictions with stringent data protection laws. Ultimately, these companies must adopt a principled stance, using their power to champion privacy and human rights in the face of authoritarian overreach.