Journal of Law & Social Studies (JLSS)
Volume 8, Issue 2, pp 221-234
www.advancelrf.org

Public Perceptions of Privacy, Data Protection, and Cybercrime Vulnerability in Pakistan: An Empirical Inquiry

Uzair Junaid
Lecturer, University Gillani Law College, Bahauddin Zakariya University, Multan
Email: uzairjunaid@bzu.edu.pk

Abstract
Rapid digitization has expanded the attack surface through which personal information can be harvested, traded, and misused. Because most consumer devices and platforms are not designed with privacy safeguards built in, and because users routinely accept terms of service without reading them, commercial intermediaries and criminal networks alike gain access to troves of personal data. This study examines how Pakistani internet users understand and respond to questions of privacy, data protection, and cybercrime, drawing on two original surveys: a 2019 pilot among educated residents of Islamabad and a larger national survey carried out in 2023. The findings show that awareness of data protection terminology and legal frameworks remains shallow even among literate respondents, although familiarity with specific protective tools such as two-factor authentication is comparatively high. Roughly one in three respondents reported having been victimized by some form of cybercrime, a proportion likely to understate the true scale of the problem once Pakistan's large unschooled population is taken into account. The paper situates these findings within the broader scholarship on data localization, surveillance, and digital governance, and argues that the absence of a functioning data protection statute leaves Pakistani citizens with few institutional remedies when their information is compromised.

Keywords: Cybercrime victimization, Digital literacy, Internet governance, Personal Data Protection Bill, Data breach, South Asia, Information privacy, Cybersecurity awareness

1. Introduction

The expansion of information and communication technologies (ICTs) has reorganized how economic value, political influence, and personal information move across borders. Cross-border data flows are now treated as an engine of growth: they lower the transaction costs of trade, allow firms of every size to operate in distant markets, and accelerate the circulation of research and innovation. McKinsey & Company (2023) estimated that global data flows already added the equivalent of $2.8 trillion to world GDP by 2014, a figure that has almost certainly grown since. Yet the same infrastructure that enables this connectivity also exposes individuals to forms of intrusion that were previously unimaginable. The disclosures made by Edward Snowden about American signals-intelligence programs, together with the Cambridge Analytica affair, pushed questions of personal data protection from a specialist concern into mainstream political debate (Sargsyan, 2016). Governments have responded unevenly. Some have pursued data localization requiring that data concerning citizens or residents be collected, processed, and in some cases stored within national borders before any international transfer occurs (Sharma & Bhandari, 2023). The motivations behind localization are mixed: deterring foreign intelligence services from monitoring domestic networks, nurturing local digital industries, strengthening the hand of domestic law enforcement, and, more controversially, tightening political control over the circulation of information. Chander and Lê (2015) capture this tension memorably, warning that localization can collapse into an equation of "censorship plus localization equals total control," since a state that can compel data to remain within reach is also a state with enhanced capacity to surveil its own population.

The stakes are not only political. In economic terms, data has been described as the resource that now plays the role oil once did in industrial economies (Palmer, 2006), except that, unlike oil, data is not depleted by use; it accumulates. Where no data protection regime exists, both domestic and foreign firms can exploit behavioral data for profiling and targeted advertising with little restraint, building commercial portraits of individuals that may be more detailed than what their own families know (The Irish Times, 2018). In the political sphere, unregulated access to personal data has been shown to distort electoral competition: during the 2016 United States presidential campaign, data harvested from roughly 87 million Facebook profiles via Cambridge Analytica was used to micro-target voters with partisan messaging (Cadwalladr & Graham-Harrison, 2018; Vox, 2018). Pakistan occupies an uneasy position within this global picture. With an internet-using population estimated at around 127 million, more than half of the country's residents, Pakistan still lacks an enacted data protection statute (Pakistan Telecommunication Authority, 2023). Legislative drafts have circulated since 2018 without reaching the floor of parliament in finished form, while lawmakers themselves often display limited familiarity with the issues such legislation is meant to address (Privacy International, 2023). Compounding this domestic vacuum, Pakistani networks have repeatedly been targets of foreign surveillance. Leaked documents analyzed by The Guardian showed that the National Security Agency's Boundless Informant tool recorded Pakistan as having among the highest volumes of intercepted telephony metadata of any country in the dataset, with billions of records of dialed-number traffic captured through the Fairview program in a single month (The Guardian, 2013a). Separate reporting indicated that tens of millions of Pakistani call records were processed through the SKYNET program (The Guardian, 2013a), while declassified materials suggest authorization was granted in 2010 for surveillance directed at Pakistani governmental and political targets (Federal Aviation Administration, 2010). Britain's GCHQ has also been implicated: investigative reporting by Greenwald (2015) described computer-network-exploitation operations that reportedly gave the agency access to “almost any user of the internet inside Pakistan” before 2008.

Domestic vulnerabilities compound these external threats. Surfshark's data-breach tracking placed Pakistan 51st globally, with close to 20 million email accounts and roughly 58 million discrete data points compromised since 2004, figures that, while substantial, are dwarfed by neighboring India's reported 293 million breached accounts and 1.1 billion compromised data points (Surfshark, 2023). Stolen financial data routinely surfaces on dark-web marketplaces, enabling fraudulent transactions using compromised debit cards (Siddiqui, 2018), and there have been documented cases of citizens being induced to sell their identity documents, as well as bank and telecom employees colluding with fraud networks to siphon funds from unsuspecting account holders (Fareedi, 2017). Against this backdrop, the present study set out to map how ordinary Pakistanis, first an educated subset, later a broader national sample, understand and act on questions of privacy, data protection, and cybercrime risk. Rather than attempting an exhaustive survey of every dimension of digital privacy, the instrument concentrated on a focused set of questions judged most likely to affect individuals in their daily use of technology. A pilot study of 157 respondents was conducted in Islamabad in late 2019, during a period when the Personal Data Protection Bill 2018 was still under public discussion; that bill was subsequently superseded by drafts in 2020 and 2021, the latter receiving federal cabinet approval in February 2022 without becoming law (Government of Pakistan, Finance Division, 2023). A second, larger survey of 455 respondents was administered nationally between April and June 2023, by which point the Ministry of Information Technology and Telecommunication had circulated a further revised draft, the Personal Data Protection Bill 2023, itself still pending vetting (Amin, 2023; Shahid, 2023). Comparing the two waves allows the analysis to speak not only to the present state of awareness but also to how that awareness has, or has not, shifted over roughly four years of legislative drift.

2. Literature Review

Scholarship on cross-border data governance can be loosely divided between skeptics of data localization and its defenders, with a growing middle ground that treats the dichotomy as overly

simple. Cory (2017) is representative of the skeptical position, arguing that the justifications typically offered for localization rarely withstand scrutiny: because international trade increasingly depends on the unimpeded movement of data, states that erect localization barriers chiefly raise costs for their own economies. Chander and Lê (2015) go further, contending that localization measures often fail even on their own terms; they neither reliably improve privacy nor security, and they do little to insulate data from foreign surveillance, while simultaneously equipping governments with tools for domestic control. Their alternative is to strengthen substantive privacy and security protections rather than fragment the internet along national lines. Other scholars resist treating localization as a single, evaluable policy. Panday and Malcolm (2018) argue that the phenomenon needs to be understood as the product of multiple, often competing actors security agencies, domestic industry, civil society, and foreign investors whose interests do not point in a single direction, with the result that localized governance arrangements are likely to remain a durable feature of the global data landscape even as they sit uneasily alongside the internet's borderless architecture. Writing from a Chinese context, Feng (2019) suggests that emerging regimes can usefully borrow the common structural elements found across established Western data protection statutes while still tailoring substantive content to local conditions; Zhang (2018) likewise acknowledges the developmental benefits of big data while insisting that those benefits cannot be separated from new categories of information-security risk. The Centre for Internet and Society (2019) proposes a more functional test, suggesting that policy should turn on what categories of data genuinely implicate national interest rather than treating all data as equally sensitive, a position echoed in Hong's (2019) “reasonable limit theory,” which ties cross-border transfer to a proportionate security-assessment process rather than blanket restriction.

A further strand of literature looks for compromise mechanisms that preserve data flows while still protecting individuals. The GSMA (2018) recommends that states begin with a candid appraisal of where they currently stand on data privacy before committing to a destination, arguing that well-designed privacy rules can themselves become an enabler of cross-border flows by building the trust on which a digital economy depends. Mattoo and Meltzer (2018) propose a converse allocation of responsibility, in which regulators in the country receiving data assume legal obligations to protect the privacy of foreign data subjects, thereby removing the need for the sending state to restrict flows in the first place. Sun (2023) notes that, notwithstanding the surge in demand for cross-border data exchange during the COVID-19 period, the field still lacks settled definitions for basic terms such as “personal data” or “cross-border data flow,” even as instruments like the Comprehensive and Progressive Agreement for Trans-Pacific Partnership have begun to function as templates for subsequent trade agreements by permitting localization only for “legitimate public policy objectives.” Literature specific to Pakistan is comparatively thin. Hayat (2007) traces the country's earliest interest in data protection legislation to a desire to position Pakistan as an attractive destination for outsourced business-process work by aligning loosely with the European Union's legal framework, while also situating privacy within an Islamic ethical tradition that long predates contemporary technology debates. Privacy International (2023) finds that, in the continued absence of comprehensive legislation, data privacy in Pakistan is governed only indirectly, through a patchwork of statutes never designed with this purpose in mind. Ali (2023) frames data protection as inseparable from digital security more broadly, arguing that because privacy and data protection law is necessarily anchored in national sovereignty even as cyber threats operate transnationally, Pakistan requires robust domestic rules that simultaneously shield citizens' data and harden the state against external intrusion. The Association for Progressive Communications (2023) contends that legislative inertia carries real costs: it discourages foreign firms from outsourcing services to Pakistan and erodes public trust in government data stewardship, while a workable statute would yield both economic and reputational benefits.

Several Pakistani commentators have engaged critically with successive drafts of the data protection bill. Khilji (2018) welcomes elements of the original 2018 draft but flags the absence of provisions governing data processing by state institutions and remedies against state surveillance, concerns the

Digital Rights Foundation has echoed in pointing to vague drafting and an awkward overlap with the Prevention of Electronic Crimes Act 2016. Mahmood (2018, 2021) raises two further concerns: that data hosted on servers in other South Asian states could expose Pakistan to corporate or state-level espionage, and that successive drafts have lacked sector-specific scope and mandatory breach-reporting requirements. Other commentators note that draft legislation has tended to leave private platforms largely unaccountable for breaches on their systems despite the historical record of such breaches compromising personal safety and democratic processes (Baig, 2021; Nawaz, 2021). Prasad and Aravindakshan (2021) conclude that Pakistan's constitutional protection for privacy has not translated into effective constraints on state or commercial exploitation of personal data. Comparative work by Javed, Salehin, and Shehab (2020) finds Pakistani websites' privacy compliance trailing comparable Indian sites but exceeding Bangladeshi sites, while Media Matters for Democracy (2021) concludes that the 2020 draft bill continued to privilege state interests over citizens' privacy. Erie and Streinz (2021) situate Pakistani data governance within a regional "Beijing Effect," arguing that the China–Pakistan Economic Corridor has encouraged convergence between Chinese and Pakistani approaches favoring state access over individual protection. Taken together, this body of work has concentrated overwhelmingly on the legislative and institutional dimensions of data protection in Pakistan. What remains largely unexamined is how ordinary citizens, the population such legislation is ultimately meant to protect, actually understand privacy, recognize threats, and adopt, or neglect, protective behaviors. The present study addresses that gap.

3. Methodology

The research instrument combined six demographic items with eleven substantive questions covering experience of cybercrime, knowledge of cybersecurity terminology, and attitudes toward privacy and data protection (the full instrument is reproduced in the appendix). Two distinct rounds of data collection were carried out four years apart, allowing the analysis to track change over a period that spans several legislative drafts. The pilot round was conducted in Islamabad in November and December 2019, a period constrained by the early effects of the COVID-19 pandemic on in-person research. Because the aim of this round was specifically to gauge how an educated, civically engaged population perceives these issues, the questionnaire was distributed using purposive sampling: it was emailed to students and graduates of Islamabad's five public-sector universities and to other respondents with at least some tertiary education known personally to the research team, with a snowball mechanism inviting initial respondents to pass the survey on to similarly qualified contacts. A parallel distribution channel used WhatsApp, accompanied by an explanatory note on the survey's purpose; respondents less comfortable in English were assisted in completing the form. Reliance on email distribution proved costly in practical terms, yielding a response rate of only 7.6 percent, a result that informed methodological changes for the subsequent national survey.

The second round, fielded nationally between April and June 2023 after pandemic-era restrictions had lifted, was designed to be broadly representative along gender and provincial lines, drawing 455 completed responses. Rather than relying on email, the team adopted a snowball strategy rooted in personal contacts across different regions of the country, with each initial contact's networks of friends and family progressively expanding the pool of respondents. To guard against the spam and fraudulent responses that commonly affect online surveys (Teitcher et al., 2015), several safeguards were layered together: CAPTCHA verification to filter automated submissions, a cap on the number of responses permitted from a single IP address, email verification to discourage the use of disposable addresses, and a post-collection review pass that screened for inconsistent answers, repetitive response patterns, or incomplete submissions. Before fielding, the questionnaire was reviewed by an academic expert and an industry professional, whose suggested revisions were incorporated, and it was piloted several times internally. Where respondents proved unfamiliar with technical terms, including ride-hailing apps' "number masking" feature and the Truecaller application, brief explanations were provided so that responses reflected genuine comprehension rather than guesswork. The final instrument comprised seventeen multiple-choice items and a single open-ended

question, administered through Google Forms and typically completed within two to three minutes. It is important to register a limitation that the authors themselves flag: because both survey rounds depended on literacy and internet access for participation, neither captures the views of Pakistan's unschooled population, which the authors estimate at roughly 42 percent of the total population. Existing research associates lower educational attainment with heightened vulnerability to cybercrime (Ashraf et al., 2023), which suggests that the cybercrime-victimization rates reported below are, if anything, conservative relative to the population as a whole.

4. Profile of Respondents

The national sample of 455 respondents was close to evenly split by gender, with men accounting for 52 percent and women 48 percent. Respondents aged 18 to 30 formed the largest age bracket by a wide margin, followed by those aged 31 to 45, reflecting the youthful skew of Pakistan's internet-using population more broadly. Educational attainment was concentrated at the upper end of the scale: graduates made up close to seven in ten respondents, with postgraduates contributing a further 17.8 percent, while those with less than an intermediate-level education together accounted for barely more than one percent of the sample a composition that should be read as a description of who completed the survey rather than as evidence that Pakistan's population is this highly educated. Provincial representation tracked the 2017 census fairly closely but over-represented Punjab, including Islamabad, relative to its national population share, while under-representing Sindh, Khyber Pakhtunkhwa, and the former Federally Administered Tribal Areas. Table 1 sets out the comparison.

Table 1: *Demographic Composition of the 2023 National Survey Sample Relative to the 2017 Population Census*

Variable	Category	Survey Share (N = 455)	2017 Census Share
Academic qualification	Under Matric	0.2%	—
	Matric	0.9%	8.1%
	Intermediate	11.6%	3.8%
	Graduate	69.5%	4.0% (Graduate & above)
	Post-Graduate	17.8%	—
Province/region	Punjab	37.6%	52.9%
	Islamabad	26.2%	0.9%
	Sindh	15.2%	23.0%
	Khyber Pakhtunkhwa	12.7%	14.7%
	Balochistan	6.2%	5.9%
	Erstwhile FATA	2.2%	2.4%

Monthly income	Unemployed	54.1%	—
	Below Rs. 17,500	4.8%	—
	Rs. 17,501–50,000	13.8%	—
	Rs. 50,001–100,000	14.3%	—
	Rs. 100,001–200,000	7.5%	—
	Above Rs. 200,000	5.5%	—

A majority of respondents reported being unemployed at the time of the survey, with students likely accounting for a significant share of this category given the age profile of the sample; among those reporting income, the Rs. 50,001–100,000 band, which can reasonably be characterized as middle-income in the Pakistani context, contributed the largest single group.

5. Results

5.1 Exposure to Cybercrime

Respondents were presented with a list of cybercrime categories adapted from the Federal Bureau of Investigation's Internet Crime Complaint Center taxonomy (Federal Bureau of Investigation, 2019) and asked to indicate which, if any, they had personally experienced. Hacking was the most commonly reported offense, affecting 27 percent of respondents, followed closely and equally by cyberbullying and cyber-harassment or cyberstalking, each cited by 25 percent. Charity fraud, financial fraud, and non-payment or non-delivery fraud were each reported by 22 percent of respondents, while malware or virus infection and phishing-related attacks (encompassing phishing, vishing, smishing, and pharming) were each reported by 21 percent. Investment fraud affected 18 percent, and identity theft 15 percent. The clustering of multiple offense categories around the 20–25 percent range suggests that victimization in this sample is not concentrated in a single dominant offense type but is instead spread fairly evenly across several distinct attack vectors.

5.2 Sharing of Personal Data Items

Respondents were asked which of thirteen categories of personal information they had shared, in either private or public mode, on social media platforms. Date of birth was the most widely shared item, disclosed by 77 percent of respondents, followed by age (67 percent), phone number (63 percent), legal name (63 percent), and marital status (51 percent). Ethnic, national, or religious origin was shared by 42 percent, residential address by 34 percent, and computerized national identity card (CNIC) number and sexual orientation each by 22 percent, the same proportion that shared a landline telephone number. Information about parents, spouses, or children was shared by 15 percent, payment-card numbers by 12 percent, and passport numbers by only 3 percent. A small minority, 7 percent, reported never having shared any of the listed items, while a similarly small group, 4 percent, reported having shared all of them. When asked whether any of this information had ever been leaked online, 84 percent answered that it had not, leaving 17 percent who reported some form of leak. A related but distinct question asked whether respondents had ever been the victim of a personal data breach specifically: here, 27 percent answered affirmatively against 73 percent who had not. The modest gap between these two figures a slightly lower rate of acknowledged “leakage” versus “breach” likely reflects differing interpretations of the two terms by respondents rather than two genuinely distinct phenomena, and points to a broader conceptual fuzziness around what counts as a data compromise.

5.3 Adoption of Privacy-Protective Behaviors

The survey probed several concrete protective behaviors. Regarding the number-masking feature offered by ride-hailing applications such as Careem and Uber, only 9 percent of respondents reported always using it, and 15 percent reported using it often, while 31 percent used it only occasionally and 46 percent reported never using it at all, meaning a clear majority either rarely or never takes advantage of a feature explicitly designed to protect their phone number from drivers. By contrast, adoption of two-factor authentication was comparatively high, with 85 percent of respondents reporting that they use it, against 15 percent who do not. Paid VPN usage was reported by 26 percent of respondents, a figure the authors link to the political circumstances surrounding the survey period: Pakistan's mobile broadband and major social media platforms were suspended for four days in May 2023 amid nationwide unrest following the arrest of former Prime Minister Imran Khan (Arab News PK, 2023), a period during which VPN demand in Pakistan was reported to have spiked by 1,329 percent in a single day (Top10VPN, 2023). Knowledge of how to report a cybercrime was held by 52 percent of respondents, leaving 48 percent without a clear sense of the appropriate reporting channel. Reuse of a single email address across both social and non-social activities was reported by 71 percent of respondents, a practice that increases exposure to identity-linked attacks should any one account be compromised. Just over half of respondents, 53 percent, reported that they check the destination of a URL before clicking on a link shared with them, leaving 47 percent who do not routinely perform this basic precaution. On the question of session hygiene, only 22 percent reported signing out of social media accounts after use, while 78 percent remained signed in, and 76 percent specifically acknowledged remaining logged into social platforms while engaged in unrelated browsing activity, a practice that increases exposure to cross-site tracking and session-hijacking risks. Finally, regarding the Truecaller application, which builds a crowd-sourced database linking phone numbers to identities, only 17 percent of respondents reported having it installed, with the remaining 83 percent declining to use it, a pattern broadly consistent with the privacy concerns that have been raised about the app's data-collection model in other South Asian markets (Singh, 2022).

5.4 Awareness of Privacy and Data Protection Terminology

Respondents were asked which of nine terms related to privacy and data protection they recognized. “Data privacy” itself was the most widely recognized term, followed by two-factor authentication at 77 percent and “personal data protection” at 64 percent. Recognition fell sharply for more technical or legally specific terms: HTTP cookies were recognized by 51 percent, virtual private networks by 35 percent, “personal data processing” by 26 percent, the General Data Protection Regulation (GDPR) by 22 percent, and “data hygiene,” the least recognized term, by only 17 percent. This pattern of high recognition of consumer-facing security features alongside low recognition of the legal and regulatory vocabulary of data protection recurs throughout the survey and is discussed further below.

5.5 Policy Attitudes

Respondents were asked several questions probing attitudes toward state surveillance and data access. A majority, 58 percent, agreed that the state should be permitted to surveil every citizen in the interest of social security, while 42 percent disagreed. When the question shifted from general surveillance to “unfettered” state access to citizens' personal data specifically, support dropped sharply: only 28 percent favored such access, against 72 percent opposed, suggesting that respondents distinguish between surveillance framed as a collective security measure and a more openly framed grant of unrestricted state access to personal information. On willingness to pay for privacy, 74 percent of respondents indicated they would be willing to pay for a digital service if the provider guaranteed that no personal data would be collected as a condition of using it. Among those who specified an amount, 49 percent indicated they would pay no more than Rs. 1,000 a month for such a guarantee, 32 percent would pay between Rs. 1,000 and Rs. 2,000, 13 percent between Rs. 2,001 and Rs. 5,000, 4 percent between Rs. 5,001 and Rs. 10,000, and the remaining 2 percent more than Rs. 10,000 indicating that, while willingness to pay something is widespread, willingness to pay substantial sums is confined to a small minority. Two further questions tested common misconceptions. Thirty-three percent of

respondents agreed that privacy is fundamentally a "Western construct," against 67 percent who disagreed, a finding the authors connect to scholarship situating privacy within Islamic ethical and legal tradition well before its contemporary technological framing (Hayat, 2007). Asked whether privacy and data protection are interchangeable terms, 52 percent answered that they are, against 48 percent who correctly distinguished them, privacy referring to freedom from unwanted observation or judgment, data protection referring to the legal regulation of how personal information is processed.

5.6 Influences on Privacy Attitudes

An open-ended question asked respondents to identify the source that had most shaped their views on privacy and data protection. Mainstream media was cited most often, by 11 percent, followed by friends and by films or television programs, each cited by 10 percent. Family was cited by 7 percent, social media and teachers each by 6 percent, the internet generally by 3 percent, university coursework by 3 percent, and formal educational qualifications by 2 percent, while 15 percent of respondents named multiple influences rather than a single source. Specific software tools mentioned included mobile security applications and the Firefox browser, and respondents named civil-society organizations including Media Matters for Democracy and the Digital Rights Foundation as influences on their thinking. Among films and television programs, respondents most frequently mentioned the documentary Terms and Conditions May Apply, the film Snowden, and the series Mr. Robot; several respondents also credited specific technology commentators and cybersecurity educators as influences.

6. Critical Discussion

The pattern that emerges across these results is one of partial, unevenly distributed awareness rather than either comprehensive ignorance or genuine literacy. Respondents recognize and adopt the protective tools actively promoted to them by technology companies, two-factor authentication chief among them, but show much weaker familiarity with the legal and conceptual vocabulary of data protection as a regulatory field. This gap is consistent with the absence of any sustained government effort to build public awareness; unlike two-factor authentication, which firms such as Google and Meta have spent years actively nudging users toward (Lawler, 2021; Page, 2021), no comparable institutional actor in Pakistan has taken responsibility for explaining what data protection law is or what recourse exists when it is violated. Comparative survey data from Statista (2019) found that 60 percent of Indian respondents and 46 percent of Chinese respondents reported being at least somewhat aware of their countries' data protection rules; even allowing for differences in survey design, the Pakistani figures recorded here 22 percent aware of GDPR, 17 percent aware of "personal data processing" or "data hygiene" suggest a meaningfully lower baseline of regulatory literacy. The confusion between privacy and data protection as concepts, endorsed by just over half the sample, is not a trivial semantic slip. Privacy concerns the individual's interest in being free from unwanted observation or judgment; data protection concerns the legal architecture governing how an organization may lawfully collect, process, and retain personal information. Where citizens conflate the two, they are less likely to recognize that the absence of a data protection statute represents a distinct and addressable institutional failure, separate from whatever informal social norms around privacy may already exist. Similarly, the substantial minority who regard privacy itself as an imported "Western" idea sit awkwardly alongside the country's own legal and religious traditions, which scholars such as Hayat (2007) trace to Quranic and broader Islamic jurisprudential sources predating any contemporary international framework; this suggests that the misconception in question is less a reasoned position than a byproduct of how privacy discourse has been imported and popularized through globalized digital culture rather than grounded in indigenous tradition.

The relatively high rate of two-factor-authentication adoption (85 percent) should not be read uncritically as evidence of strong security practice, since the survey did not ask whether respondents had enabled the feature across all their accounts or only a subset; future work could usefully disaggregate this further. Paid VPN adoption, at 26 percent, is striking given that nearly three-quarters

of the sample fell into lower income brackets earning at or below Rs. 50,000 a month, and becomes more explicable once situated against the political backdrop of the survey period, when state-imposed restrictions on mobile broadband and major platforms drove a documented spike in VPN demand nationally (Arab News PK, 2023; Top10VPN, 2023). Atlas VPN's regional index for 2021 had already identified Pakistan as having the highest rate of VPN usage in South Asia, ahead of India and Sri Lanka (Atlas VPN, 2021), suggesting that VPN adoption in Pakistan is driven less by a generalized data-protection ethic than by the specific and recurring experience of state-imposed internet censorship. Several behavioral findings point toward heightened, largely unrecognized exposure to identity-based and phishing-related attacks. Roughly seven in ten respondents reuse a single email address across social and non-social activity, a practice that compounds the damage any single account compromise can cause; just under half do not routinely check a link's destination before clicking it; and the large majority remain signed into social accounts during unrelated browsing sessions. This combination, alongside low Truecaller adoption and low reporting literacy, paints a picture of a user base that is, on balance, more reactive than preventive in its security posture, consistent with research linking lower digital literacy to heightened cybercrime vulnerability (Ashraf et al., 2023) and with the broader claim that a large share of everyday cyber threats are avoidable through basic user awareness (Sanger, 2019).

The finding that three-quarters of respondents share their date of birth and roughly two-thirds share their phone number and legal name on social media, set against the finding that roughly one in five has experienced identity theft or had their CNIC number circulate publicly, underscores a disconnect between disclosure behavior and risk awareness. This disconnect is not unique to Pakistan, but it carries particular weight in a context where no statutory mechanism exists for citizens to seek redress once such information has been misused. The 58 percent of respondents willing to accept blanket state surveillance “for social security” purposes is also worth dwelling on critically: this figure sits in tension with the much lower, 28 percent, support for “unfettered” state access to personal data, suggesting that framing matters considerably to how citizens evaluate state power over their information a finding consistent with broader research on how surveillance measures introduced under public-health or security framing, including those deployed during the COVID-19 pandemic in South and Southeast Asia, have sometimes been repurposed for purposes such as monitoring planned protests (Sombatpoonsiri & Mahapatra, 2021). Pakistan's comparatively weak position in cross-national rankings reinforces these survey findings. The Stevens Institute of Technology's internet-privacy ranking placed Pakistan 61st among 70 countries assessed (Stevens Institute of Technology, n.d.), while the International Telecommunication Union's Global Cybersecurity Index 2020 ranked Pakistan 79th of 194 countries on overall cybersecurity commitment, a composite measure that includes data-protection capacity among its component pillars (International Telecommunication Union, 2021). These rankings corroborate, at the institutional level, what the survey data suggest at the level of individual awareness and behavior: Pakistan lags behind regional and global peers not because its citizens are uniquely careless, but because the legal, regulatory, and educational scaffolding that elsewhere supports more informed digital behavior has simply not been built.

7. Conclusion and Recommendations

This study set out to establish an empirical baseline for understanding how Pakistani internet users perceive privacy, data protection, and cybercrime risk, comparing an educated subset surveyed in 2019 with a more broadly representative national sample surveyed in 2023. The findings indicate that awareness remains shallow, particularly with respect to the legal and regulatory dimensions of data protection, even though awareness of specific consumer-facing security tools is comparatively strong. Close to one in three respondents reported having been a victim of some form of cybercrime, and the true population-wide figure is likely higher still once Pakistan's substantial unschooled population, excluded from this sample by design, is taken into account. Protective behavior is similarly inconsistent: high uptake of two-factor authentication coexists with widespread reuse of email addresses, limited URL-checking discipline, and low awareness of cybercrime-reporting channels.

These patterns cannot be attributed solely to individual choices. They reflect, in significant part, the absence of sustained government investment in public awareness around data protection, and the continued non-enactment of a comprehensive data protection statute despite successive draft bills since 2018. Pakistan's National Cyber Security Policy 2021 explicitly identified the cultivation of a mass cyber-aware culture as a policy deliverable, yet implementation has so far been limited; a step in the right direction came in May 2023, when the National Parliamentary Taskforce on Sustainable Development Goals signaled interest in working with educational institutions to build awareness of cybercrime and of the Prevention of Electronic Crimes Act 2016. Civil-society organizations, including Media Matters for Democracy and the Digital Rights Foundation, have continued to fill part of this gap through research and advocacy, but their reach is necessarily limited without a corresponding government commitment.

Several recommendations follow from these findings. First, the enactment of a comprehensive data protection law, broadly aligned with internationally recognized benchmarks such as the GDPR while reflecting Pakistan's own legal and constitutional context, would give citizens a concrete mechanism for redress and would bring Pakistan into closer alignment with the more than 130 countries that the United Nations Conference on Trade and Development (2024) reports have already enacted such legislation. Second, given how strongly two-factor-authentication adoption tracked active promotion by technology firms, similarly sustained public-information campaigns run jointly by government agencies and the private sector could plausibly raise awareness of cybercrime-reporting channels and basic protective practices such as link verification and credential hygiene. Third, the introduction of compulsory privacy and data protection content within university curricula, particularly for students pursuing technology-related degrees, alongside the broader adoption of “privacy by design” as a pedagogical and engineering principle, would help close the gap between technical literacy and regulatory literacy that this survey has identified. Finally, future research should prioritize reaching Pakistan's unschooled and rural populations, whose perspectives and levels of exposure to cybercrime this study, by virtue of its sampling method, was unable to capture, but who are likely to be at least as vulnerable, and quite possibly more so, than the educated respondents surveyed here.

References

Ali, J. (2023, June 26). Data protection law in Pakistan: Policy recommendations by DRF. Digital Rights Foundation. https://digitalrightsfoundation.pk/data-protection-law-in-pakistan-policy-recommendations-by-drf/

Amin, T. (2023, June 24). Personal data protection bill finalised. Brecorder. https://www.brecorder.com/news/40243443

Arab News PK. (2023, June 27). Businesses in Pakistan bear the brunt of mobile internet suspension amid protests. Arab News. https://arab.news/vyjc4

Ashraf, A., König, C. J., Javed, M., & Mustafa, M. (2023). " Stalking is immoral but not illegal": Understanding Security, Cyber Crimes and Threats in Pakistan. In the *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)* (pp. 37-56).

Association for Progressive Communications. (2023). Data protection in Pakistan. https://www.apc.org/sites/default/files/Data_Protection_in_Pakistan.pdf

Atlas VPN. (2021). VPN usage by country 2023. https://atlasvpn.com/vpn-adoption-index

Baig, A. (2021). Privacy in the digital age. The News on Sunday. https://www.thenews.com.pk/tns/detail/568763-privacy-digital-age

Cadwalladr, C., & Graham-Harrison, E. (2018, March 17). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian. http://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Centre for Internet and Society. (2019). The localisation gambit: Unpacking policy measures for sovereign control of data in India. https://cis-india.org/internet-governance/resources/the-localisation-gambit.pdf

Chander, A., & Lê, U. P. (2015). Data nationalism. *Emory Law Journal*, *64*(3).

Cory, N. (2017). *Cross-border data flows: Where are the barriers, and what do they cost?*. Information Technology and Innovation Foundation. https://www2.itif.org/2017-cross-border-data-flows.pdf

Erie, M. S., & Streinz, T. (2021). *The Beijing effect: China's "Digital Silk Road" as transnational data governance*. *New York University Journal of International Law and Politics, 54*(1), 1–58. https://ssrn.com/abstract=3810256

Fareedi, T. (2017, June 26). Cybercriminal network expanding fast. The Express Tribune. https://tribune.com.pk/story/2085145/cybercriminal-network-expanding-fast

Federal Aviation Administration. (2010). FAA FG Cert 2010 exhibit F: Foreign power list. https://s3.documentcloud.org/documents/1211015/faa-fg-cert-2010-a-exhibit-f-foreign-power-list.pdf

Federal Bureau of Investigation. (2019). 2018 Internet Crime Report. Internet Crime Complaint Center. https://www.fbi.gov/news/stories/ic3-releases-2018-internet-crime-report-042219

Feng, Y. (2019). The future of China's personal data protection law: challenges and prospects. *Asia Pacific Law Review*, *27*(1), 62-82.

Government of Pakistan, Finance Division. (2023). Pakistan Economic Survey 2021–22. https://www.finance.gov.pk/survey_2022.html

Greenwald, G. (2015, June 22). Spies hacked computers thanks to sweeping, secret warrants. The Intercept. https://theintercept.com/2015/06/22/gchq-reverse-engineering-warrants/

GSMA. (2018). Regional privacy frameworks and cross-border data flows: How ASEAN and APEC can protect data and drive innovation. https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows_Full-Report_Sept-2018.pdf

Hayat, M. A. (2007). Privacy and Islam: From the Quran to data protection in Pakistan. *Information & Communications Technology Law*, *16*(2), 137-148.

Hong, Y. (2019, June 10). *Construction of the framework for security review of the cross-border data flow under the Cyber Security Law in the balance of security and development*. SSRN. https://doi.org/10.2139/ssrn.3401610

International Telecommunication Union. (2021). Global Cybersecurity Index 2020. https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

Javed, Y., Salehin, K. M., & Shehab, M. (2020). A study of South Asian websites on privacy compliance. *IEEE Access*, *8*, 156067-156083.

Khilji, U. (2018). Data protection law. DAWN. https://www.dawn.com/news/1455963

Lawler, R. (2021, October 5). Google is about to turn on two-factor authentication by default for millions of users. The Verge. https://www.theverge.com/2021/10/5/22710421/google-security-2fa-inactive-account-management

Mahmood, Z. (2018). Why Pakistan needs a cyber army? Global Village Space. https://www.globalvillagespace.com/why-pakistan-needs-a-cyber-army/

Mattoo, A., & Meltzer, J. P. (2018). International data flows and privacy: The conflict and its resolution. *Journal of International Economic Law*, *21*(4), 769-789.

McKinsey & Company. (2023). The US economy: An agenda for inclusive growth. McKinsey Global Institute.

Media Matters for Democracy. (2021). Protecting the data: A comparative analysis of Pakistan's Personal Data Protection Bill, 2020. https://mediamatters.pk/wp-content/uploads/2021/02/Comparative-Analysis-of-Personal-Data-Protection-Bill-2020.pdf

Nawaz, Q. (2021). No more delays: Need for data protection regulations in Pakistan. Hilal. https://www.hilal.gov.pk/eng-article/detail/MjA5Mw==.html

Page, C. (2021, December 2). Facebook is making two-factor mandatory for high-risk accounts. TechCrunch. https://techcrunch.com/2021/12/02/facebook-two-factor-mandatory/

Pakistan Telecommunication Authority. (2023). Telecom indicators. https://www.pta.gov.pk/en/telecom-indicators

Palmer, M. (2006). Data is the new oil. ANA Marketing Maestros. https://ana.blogs.com/maestros/2006/11/data_is_the_new.html

Panday, J., & Malcolm, J. (2018). The political economy of data localization. *Partecipazione e conflitto*, *11*(2), 511-527.

Prasad, S. K., & Aravindakshan, S. (2021). Playing catch-up–privacy regimes in South Asia. In *The Right to Privacy Revisited* (pp. 83-120). Routledge.

Privacy International. (2023). State of privacy: Pakistan. https://privacyinternational.org/state-privacy/1008/state-privacy-pakistan

Sanger, D. E. (2019). *The perfect weapon: War, sabotage, and fear in the cyber age*. Crown.

Sargsyan, T. (2016). Data localization and the role of infrastructure for surveillance, privacy, and security. *International Journal of Communication*, *10*, 17-17.

Shahid, J. (2023, June 24). Senate panel directs PTA to provide telcos' income details. DAWN. https://www.dawn.com/news/1756116

Sharma, U., & Bhandari, A. (2023). How would data localization benefit India? Carnegie India. https://carnegieindia.org/2021/04/14/how-would-data-localization-benefit-india-pub-84291

Siddiqui, S. (2018). Another bank faces data theft. The Express Tribune. https://tribune.com.pk/story/2354210/another-bank-faces-data-theft-1

Singh, M. (2022). How billion-dollar caller ID app, Truecaller, knows so much about you. Rest of World. https://restofworld.org/2022/how-truecaller-built-a-billion-dollar-id-data-empire-in-india/

Sombatpoonsiri, J., & Mahapatra, S. (2021). COVID-19 intensifies digital repression in South and Southeast Asia. Carnegie Endowment for International Peace. https://carnegieendowment.org/2021/10/19/covid-19-intensifies-digital-repression-in-south-and-southeast-asia-pub-85507

Statista. (2019). Data protection and privacy rule awareness by country. https://www.statista.com/statistics/1015277/data-protection-and-privacy-rule-awareness-by-country/

Stevens Institute of Technology. (n.d.). Countries ranked by internet privacy. https://online.stevens.edu/info/countries-ranked-by-internet-privacy/

Sun, L. (2023). Overview of regulations on cross-border data flow. *Academic Journal of Science and Technology*, *8*(1), 171-176.

Surfshark. (2023). Data breach monitoring. https://surfshark.com/research/data-breach-monitoring

Teitcher, J. E., Bockting, W. O., Bauermeister, J. A., Hoefer, C. J., Miner, M. H., & Klitzman, R. L. (2015). Detecting, preventing, and responding to "fraudsters" in internet research: ethics and tradeoffs. *Journal of Law, Medicine & Ethics*, *43*(1), 116-133.

The Guardian. (2013a, June 8). Boundless Informant: NSA's secret tool to track global surveillance data. The Guardian. https://www.theguardian.com/us-news/boundless-informant

The Irish Times. (2018). What Netflix, Spotify, and YouTube know about you. https://www.irishtimes.com/culture/what-netflix-spotify-and-youtube-know-about-you-1.3444260

Top10VPN. (2023). VPN demand statistics: VPN demand surges around the world. https://www.top10vpn.com/research/vpn-demand-statistics/

United Nations Conference on Trade and Development. (2024). Data protection and privacy legislation worldwide. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

Vox. (2018). The Facebook and Cambridge Analytica scandal, explained with a simple diagram. https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram

Zhang, D. (2018, October). Big data security and privacy protection. In *8th International Conference on Management and Computer Science (ICMCS 2018)* (pp. 275-278). Atlantis Press.