Surveillance, Scandals, and Secrets: The Relevance of South Korean Government Surveillance to the Audio Leaks Case in Pakistan

Yessica Chong, GW Law's Civil and Human Rights Law Clinic

September 2025

I. Introduction

Picture this: the First Lady was on the phone discussing political party-related information. A number of political events cause friction and instability within the government. In the midst of this political turmoil, the First Lady's phone conversations are strategically leaked to the press. Sounds like the Audio Leaks Case in Pakistan, specifically the audio recordings released of Pakistani Prime Minister Imran Khan's wife, Bushra Bibi, and her private conversations.[1] Surprise! It is actually a recent series of released audio recordings of Kim Keon Hee, the wife of former South Korean President Yoon Seok-yeol. In February 2025, a phone conversation between Kim Keon Hee and a political broker was made public by a local weekly affairs magazine.[2] Although the conversations occurred before President Yoon took office in May 2022, they were likely leaked in 2025 because of the pending impeachment trials of President Yoon.[3] First Lady Kim, speaking on behalf of the then President-Elect Yoon, and the political broker

[1] Faaiza Qazi, *The Politics of Exposure: Audio Leaks and the Erosion of Privacy and Democracy in Pakistan*, Digital Privacy Rights Resource 1, 13-15 (July 2025).

[2] Lee Hyo-jin, *First lady's phone call with political broker deepens election meddling controversy*, KOREA TIMES (Feb. 25, 2025), https://www.koreatimes.co.kr/www/nation/2025/02/356_392962.html (reporting the self-proclaimed political broker, Myung Tae-kyun, was indicted for charges related to the violation of political funding law).

[3] *Id.*

were allegedly discussing the ruling People Power Party's candidate nomination process for the 2022 parliamentary by-elections.[4] These recordings confirmed allegations against Kim and President Yoon that they were involved in illegal election meddling.[5] Their release to the public further complicated the couples' legal troubles, and since then, Korea's highest court has affirmed the impeachment of President Yoon.[6]

Similarly, in Pakistan, a number of private audio recordings of high-level political actors were recently made available online, a couple of which were the subject of litigation before the Supreme Court of Pakistan.[7] In April 2023, an audio recording of Mian Najamul Saqib, son of the former chief justice of Pakistan Saqib Nisar, was leaked; in November 2023, a recording of a conversation between Bushra Bibi, former Prime Minister Imran Khan's wife, and her lawyer was released; and in November 2024, another of Bushra Bibi's phone conversations discussing politics and strategies was made public. These leaked conversations were scandalous because they touched on political and internal affairs. In particular, the recordings of Bibi's conversations were all released within the period that Bibi and former Prime Minister Khan were fighting a legal battle against bribery allegations. The resulting Audio Leaks Case, or ALC, as the joint litigation is known in Pakistan, is representative of the type of nefarious surveillance that has silenced political opponents, suppressed journalists from sharing information critical of the government, and put citizens in fear of repercussions from their online activities. The joint case of Bushra Bibi and Mian Najamul Saqib has become the leading case symbolizing the fight against State surveillance overreach in Pakistan,[8] highlighting that no one is out of reach.

What can the parallel travails of former presidents and their spouses in Pakistan and South Korea tell us about government surveillance capabilities and the abuse of such power? The two countries have walked a similar path: starting from the end of military dictatorships, digital repressive policies of the government, the use of government surveillance of civilians to further the State's interests, and now the public release of the private conversations of the wives of former heads of each State's government. This Article will present a case study of State surveillance in South Korea and draw broad comparisons between that context and the Pakistani one, of which the ALC is emblematic. It will highlight the history of the South Korean government's use of overly broad surveillance to set up a discussion of similar government surveillance practices in Pakistan. The goal is to provide a foundation for readers to better understand the issue of State surveillance and draw insight into the readers' own circumstances and needs. Specifically, the study of South Korea can help to illustrate where the ALC is headed

---

[4] *Id.*
[5] Park Chan-kyong, *Voice recordings spell out more trouble for South korea's first lady*, South China Morning Post, https://www.scmp.com/week-asia/people/article/3300392/voice-recordings-spell-more-trouble-south-koreas-first-lady; Lee Hyo-jin, *supra* note 2.
[6] Lee Hyo-jin, *supra* note 2; Yoonjung Seo, Gawon Bae, Mike Valerio, and Jessie Yeung, *South Korea's impeached president is removed from office, four months after declaring martial law*, CNN, https://www.cnn.com/2025/04/03/asia/yoon-impeachment-verdict-south-korea-intl-hnk/index.html.
[7] Qazi, *supra* note 1, at 15-17.
[8] *Id.*

within the Pakistani legal system, how it might be understood by Pakistani citizens, and how people can respond to a government that does not respect their privacy rights. Global internet freedom has been declining as authoritarian governments continue in their efforts to repress the flow of news and information, centralize State control over internet infrastructure, and create barriers to cross-border transfers of user data.[9]

The remainder of this Article proceeds as follows. Part II outlines the history of South Korean government surveillance since 1979 and its evolution to the present day. Part III then compares and contrasts the South Korean case study with the Audio Leaks Case in Pakistan, highlighting applicable insights. The ALC has highlighted the obstacles Pakistan must overcome in order to create change in the government's surveillance practices and policies: intelligence agencies with nearly unlimited surveillance powers; overly broad statutory provisions authorizing government agencies to have unlimited powers; the susceptibility of corporations to government's requests; and the nonexistence of data protection laws. The South Korean case study reveals two main factors to overcoming these obstacles: (1) extensive international and domestic media coverage of the issue; and (2) significant public mobilization, both of which are lacking in Pakistan.

II. South Korea: A Case Study of Government Surveillance

The surveillance practices used by South Korea are best understood by walking through a history of presidential administrations, paying particular attention to the evolving role intelligence agencies have played in them. Accordingly, this Part outlines the evolution of government surveillance in South Korea since 1979, exemplifying how public pressure directly affects the level of surveillance the government permits. Section A outlines the origins of how the Korean government actively began to use intelligence agencies against political opponents and dissidents. Section B then explains the evolution of public sentiment with respect to intrusive government surveillance since the end of the authoritarian government in the 1980s. Section C looks at the law that grants the government's surveillance powers today.

A. The Military Dictatorship of Chun Doo-Hwan: 1979-1988

To understand the role of South Korean intelligence agencies today, it is necessary to start with the last military dictatorship in South Korea: Chun Doo-Hwan's administration (1979-1988). Chun's authoritarian control of the government was characterized by extensive spying on political opponents and dissidents. In October 1979, President Park Chung-hee was assassinated by his own chief of intelligence services, Kim Jae-kyu.[10] Chun Doo-hwan, a major general at the time, took this period of political instability to

[9] Adrian Shahbaz et al., *Freedom on the Net 2022: Countering an Authoritarian Overhaul of the Internet*, FREEDOM HOUSE, https://freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-internet.
[10] *ON THIS DAY: 1979: South Korean President Killed*, BBC, http://news.bbc.co.uk/onthisday/hi/dates/stories/october/26/newsid_2478000/2478353.stm.

stage his own military coup and take control of the South Korean government.[11] To legitimize his rule and silence opposition, Chun authorized the detention of civilians for their "anti-State activities," which included public demonstrations against government policies.[12] South Korea's National Security Act penalized such activities, and was increasingly used to suppress domestic dissent.[13] Basements of intelligence agency buildings became well-known locations for brutal interrogations and the torture of numerous opposition party members, dissidents, and student activists.[14] Intelligence agencies also conducted surveillance of political and religious minorities as well as other dissidents. Within the National Assembly, opposition members alleged that telephone-tapping and the interception of correspondence were prevalent practices.[15] "Ruling party assembly members, government officials, and senior military officials also were subjected to this interference although they did not openly complain."[16] Under Chun's military, dictatorial intelligence agencies played a significant role in legitimizing his government power.

Chun recreated and expanded intelligence agencies to cement his military dictatorship. The Agency for National Security Planning was established in 1961 and later became known by its acronym ANSP.[17] Chun redesignated ANSP as the "principal agency for collecting and processing all intelligence."[18] The ANSP's functions were redesigned through 1981 legislation to "include the collection, compilation, and distribution of foreign and domestic information regarding public safety against communists and plots to overthrow the government."[19] In order for the ANSP to fulfill its functions, the agency was given access to all government offices and files.[20] The Army Security Command (ASC)—now known as the Defense Security Command (DSC)—was the military agency responsible for intelligence activities. Some of the ASC's responsibilities included "monitoring the military for loyalty; monitoring domestic political, economic, and social activities that might jeopardize military capabilities and national unity; [… and] detecting espionage and anticommunist law violations."[21] The ASC greatly expanded its role into domestic politics under Chun's rule.[22]

Intrusive surveillance practices and the harsh silencing of opposition voices would ultimately facilitate the fall of Chun's military dictatorship. The collaboration of truth-seeking journalists and the public's desire for change as well as international condemnation of Chun's authoritarian government would ultimately lead to Chun

---

[11] Choe Sang-Hun, *Chun Doo-hwan, Ex-Military Dictator in South Korea, Dies at 90*, The New York Times (Nov. 22, 2021), www.nytimes.com/2021/11/23/world/asia/chun-doo-hwan-dead.html.
[12] *Id.*; Andrea Matles Savada & William Shaw, South Korea: A Country Study, Library of Congress (1992), https://archive.org/details/southkoreacountr00sava_0/page/66/mode/2up.
[13] *Id.*
[14] Savada & Shaw, South Korea: A Country Study, *supra* note 12.
[15] *Id.* at 311.
[16] *Id.*
[17] *Id.*
[18] *Id*. at 312.
[19] Savada & Shaw, South Korea: A Country Study, *supra* note 12, at 312.
[20] *Id.* at 313.
[21] *Id.* at 316.
[22] *Id.*

relinquishing control to a democratic government. Two events in particular precipitated this. First, on January 14, 1987, a student activist, Park Jong-chul, died while being tortured by government authorities.[23] Park had been waterboarded after being arrested to be questioned on the whereabouts of a classmate.[24] Unlike many prior cases of torture during this period, Park's death was well-publicized by the media and reinvigorated national demonstrations seeking democratization of the country.[25] As a result, Chun agreed to hold the first democratic presidential election since 1971,[26] after Korea's almost forty years of dictatorial rule.[27]

The second precipitating event was that South Korea was set to host its first ever Olympics in Seoul in 1988. All eyes of the foreign press were on Korea, especially as the 1988 Olympics were seen as a sign of thawing Cold War tensions.[28] Moreover, hosting the Olympics was an opportunity for South Korea to showcase the remarkable development and modernization of the country since a ceasefire ended the Korean War just 35 years earlier.[29] Chun had originally planned to use the Olympics to legitimize his military dictatorship.[30] Specifically, he was hoping to use "sportswashing" to improve Korea's reputation after the Kwangju Uprising in May 1981,[31] a State-sponsored massacre orchestrated by Chun.[32] However, International Olympic Committee President Juan Antonio Samaranch made clear to the Korean government officials that the Games would be relocated if widespread turmoil continued in Korea.[33] Due to this international pressure, Chun grew reluctant to use excessive force against peaceful

---

[23] *20 years later, father still seeks truth in son's death*, HANKYOREH (Oct. 19, 2019), https://english.hani.co.kr/arti/english_edition/e_national/184219.html; Clyde Haberman, *Seoul Student's Torture Death Changes Political Landscape*, THE NEW YORK TIMES (Jan. 31, 1987) https://www.nytimes.com/1987/01/31/world/seoul-student-s-torture-death-changes-political-landscape.html.

[24] *Id.*

[25] *Id.*

[26] Tom Shorrock, *South Korea: Chun, the Kims and the constitutional struggle*, THIRD WORLD QUARTERLY 95-110, 95 (Jan. 1988), available at https://www.jstor.org/stable/3992805?seq=1.

[27] Haberman, *supra* note 23.

[28] Aloysius M. O'Neill III, *The 1988 Olympics in Seoul: A Triumph of Sport and Diplomacy*, 38 NORTH (Feb. 8, 2018), https://www.38north.org/2018/02/aoneill020818/; Staff Hanguk, *Triumph and Tragedy: How the 1988 Seoul Olympics Became a Battleground for Cold War Politics*, MILWAUKEE INDEPENDENT (Oct. 15, 2024), https://www.milwaukeeindependent.com/articles/triumph-tragedy-1988-seoul-olympics-became-battleground-cold-war-politics/#:~:text=Although%20South%20Korea%20was%20under,progress%20on%20the%20world%20stage.

[29] *Id.*

[30] *Id.*

[31] David Towriss, *Explainer: What is 'Sportwashing', and How Does it Threaten Democracy?*, INTERNATIONAL IDEA (Nov. 24, 2022), https://www.idea.int/blog/explainer-what-sportswashing-and-how-does-it-threaten-democracy (defining sportswashing as the phenomenon when an actor, particularly authoritarian heads of government, use sports to launder or improve the actor's reputation. It mainly occurs when a nation hosts or sponsors a sporting event).

[32] Chandelis Duster, *Long before this week, South korea had a painful history with martial law*, NPR (Dec. 5, 2024) https://www.npr.org/2024/12/05/nx-s1-5215788/south-korea-martial-law.

[33] Aloysius M. O'Neill III, *The 1988 Olympics in Seoul*, *supra* note 27.

demonstrators, allowing the spread of the national demonstrations which would ultimately force Chun to step down from power.[34]

With the end of Chun's power, the main intelligence agencies—ANSP and ASC—were under public pressure to cut back on their domestic political surveillance, which led to their ceasing operations in the National Assembly. The Minister of National Defense reported to the National Assembly that the ASC would eliminate the office "charged with collecting information on civilians [and curtail] its involvement in security screening of non-military government personnel." [35] According to an ASC official, however, another agency assumed the responsibility of surveilling politicians.[36] While such imperfections persisted, public outcry and media coverage nevertheless brought an end to Chun's regime and significantly curtailed the range of acceptable State surveillance for subsequent administrations.

B. State Surveillance Following Chun's Authoritarian Government

The Korean government no longer has the unlimited power of surveillance it did forty years ago, in large part because of domestic and international pressure. These changes led to increasing criminal charges against government officials that were impossible in the 80s.[37] For example, two former spy chiefs were arrested in 2006 and indicted for authorizing illegal wiretapping of government critics, politicians, and other prominent figures between 1999 and 2003.[38] But the biggest backlash to government overreach in this regard resulted in the impeachment of President Park Geun-hye in 2016: among other things, her administration's abuse of its surveillance powers turned millions of Koreans against her, and eventually became one of many reasons members of Parliament voted her out of office.[39] As a result, the government has found it harder to justify using surveillance as a tool without being scrutinized by the media and its people.

The sub-sections below will discuss how public perception of government surveillance has evolved since the end of Chun's military dictatorship, focusing on select South Korean administrations. While merely a few of many possible examples, the selected administrations are notable for the high level of public scrutiny and media coverage they have been subjected to for the use of surveillance. Importantly, this section will show how public perception of State surveillance has affected how the government and the justice system understand the gravity of the issue.

---

[34] *Id.*
[35] Savada & Shaw, South Korea: A Country Study, *supra* note 12, at 317.
[36] *Id*.
[37] *See Jail sentence demanded for Lee's aide in illegal surveillance scandal, supra* note 42; *see also* Republic of Korea 2020 Human Rights Report, U.S. Department of State, *supra* note 46.
[38] *Ex-spy chiefs arrested in South Korea*, The New York Times (Nov. 16, 2005), https://www.nytimes.com/2005/11/16/world/asia/exspy-chiefs-arrested-in-south-korea.html.
[39] *South Korea's presidential scandal*, BBC (April 6, 2018), https://www.bbc.com/news/world-asia-37971085.

1. Roh Tae Woo's Presidency (1988-1993)[40]

Two years into President Roh Tae Woo's term, soldier Yoon Seok-yang blew the whistle on the ASC's continued monitoring of civilians despite the changes enacted following the end of Chun's presidency. After starting his compulsory military service in 1990, Yoon was detained by the ASC for his student activist role in the 1980s. He received death threats from the ASC as a means of coercion to name former classmates who had also participated in anti-government demonstrations during the 1980s. After taking a personal role in arresting the classmates he named, Yoon was assigned a position at the ASC. He eventually deserted his post to hold a press conference on how the ASC had continued surveilling civilians, including the whereabouts of political opponents who would get in the way of a possible future military coup. While the government's reaction to the whistleblower's claims consisted of surface-level actions, such as changing the name of the ASC to Defense Security Command (DSC), the case increased public awareness of how government surveillance of civilians did not end with the demise of Chun's regime.

2. Lee Myung-bak's Presidency (2008-2013)[41]

In 2010, members of the ethics team from the prime minister's office were convicted of having conducted illegal surveillance of private citizens, including a businessman who had posted a video clip ridiculing then President Lee. The prosecution reopened the investigation after an official who had been indicted in 2010 claimed that he had been acting under direct orders from the Presidential Office. As a result, prosecutors unsuccessfully sought a three-year jail sentence for President Lee's former "right-hand man," but the investigation failed to clear suspicions that higher-level officials had been involved.

3. Park Geun-hye's Presidency (2013-2017)

Park Geun-hye's Presidency was riddled with allegations of abusive surveillance of civilians. Notably, after the tragic sinking of the Sewol Ferry in April 2014 that took 304 lives, 250 of which were students on a field trip,[42] it was revealed that the DSC spied on the Sewol victims' families in an effort to sway public opinion in favor of the Park administration in the wake of the tragedy.[43] Major General So Gang-won, the DSC's

---

[40] Kim Tae-kwon, *Yoon Seok-yang, the one who blew the whistle of surveillance of civilians* [translated from Korean], HANKYOREH https://www.hani.co.kr/arti/opinion/column/1160910.html; Ben McGrath, *South Korean government begins phony reform of military intelligence agency*, World Socialist Web Site (Aug. 11, 2018), https://www.wsws.org/en/articles/2018/08/11/skor-a11.html (substantiates entire paragraph).

[41] *Jail sentence demanded for Lee's aide in illegal surveillance scandal*, Korea Times (Sep. 13, 2012), https://www.koreatimes.co.kr/www/nation/2025/01/113_119822.html (substantiates entire paragraph).

[42] Sebin Choi & Dogyun Kim, *South Koreans still seek answers 10 years after Sewol ferry disaster*, Reuters (Apr. 16, 2024), https://www.reuters.com/world/asia-pacific/south-koreans-still-seek-answers-10-years-after-sewol-ferry-disaster-2024-04-16/.

[43] Shim Kyu-Seok, *Martial law probe to look at surveillance of Sewol families*, Korea JoongAng Daily (Jul. 15, 2018),

chief of staff, had used the DSC's special task force to design a political environment more favorable to President Park, in part by surveilling victims' families who were critical of the administration's botched search and rescue operations.[44] Park was impeached in December 2016 in after a massive corruption scandal revealed cult activities, influence-peddling, and leaks of classified information.[45]Subsequently, the military court sentenced General So "to one year's imprisonment for illegal surveillance of civilians."[46]

It is important to note the role that ICT companies played during the Park administration to enable or impede State surveillance. For example, after months of public criticism arising from the 2014 Sewol Ferry incident, President Park ordered a crackdown on any messages deemed insulting to her or that facilitated (in her view) false rumors.[47] Prosecutors immediately began monitoring private messages sent through Kakao Talk, a Korean messaging app similar to WhatsApp, for violations of Parks order.[48] Some users reported receiving notices informing them that their accounts had been searched.[49] In response, millions of South Koreans signed up to use Telegram, an encrypted messaging app, to stay away from government eyes.[50] As a result of this mass exodus of users, Kakao Talk's company reversed its position and stated it would no longer respond to or comply with government requests for access to users' private information.[51]

4. Moon Jae-in's Presidency (2017-2022)

During the COVID-19 Pandemic, South Korea was praised for its management of the disease. In order to identify potentially infected citizens and others to test, the government relied heavily on the use of surveillance technology, especially CCTV, bank card transactions, and mobile phone usage.[52] With this information, authorities were able to find out who an infected person had been in close contact with. The patient's movement would be compared with those of earlier patients' to pinpoint the place of

---

https://koreajoongangdaily.joins.com/2018/07/15/politics/Martial-law-probe-to-look-at-surveillance-of-Sewol-families/3050621.html.

[44] *Id.*

[45] South Korea's presidential scandal, BBC (Apr. 6, 2018), https://www.bbc.com/news/world-asia-37971085.

[46] Republic of Korea 2020 Human Rights Report, U.S. Department of State at 8, https://www.State.gov/reports/2020-country-reports-on-human-rights-practices/south-korea/.

[47] *Why South Koreans are fleeing the country's biggest social network*, BBC (Oct. 10, 2014), https://www.bbc.com/news/blogs-trending-29555331.

[48] Russel Brandom, *Surveillance drives South Koreans to encrypted messaging apps,* The Verge (Oct. 6, 2014), https://www.theverge.com/2014/10/6/6926205/surveillance-drives-south-koreans-to-encrypted-messaging-apps.

[49] *Why South Koreans are fleeing the country's biggest social network*, *supra* note 48.

[50] *Id.*

[51] *Kakao Talk says 'no' to South Korean government demands*, BBC (Oct. 14, 2014), https://www.bbc.com/news/blogs-trending-29617842.

[52] Jung Won Sonn, *Coronavirus: South Korea's success in controlling disease is due to its acceptance of surveillance*, The Conversation (Mar. 19, 2020), https://theconversation.com/coronavirus-south-koreas-success-in-controlling-disease-is-due-to-its-acceptance-of-surveillance-134068.

transmission.[53] The Infectious Disease Control and Prevention Act enables State officials to access personal information of patients, including potential ones, without a warrant.[54] Health authorities can request telecommunications companies and the National Police Agency to share the information of confirmed and potentially infected patients alike.[55] The results of the tracking were made public through government websites, smartphone apps, and emergency alerts about new local cases, helping citizens avoid hotspots of COVID-19 infections.[56] Information released by authorities included patients' daily routine, gender and age, basic description of where the patient lives, where they work or go to school, their transportation, "and all the places one stopped by."[57]

While the surveillance system undoubtedly made South Korea a leader in the response to COVID-19, the use of and reliance on surveillance systems and security technologies raised serious issues around the infringement of privacy. Concerns were voiced by the National Human Rights Commission and NGOs, and the government thereafter agreed to limit the scope of released patient information.[58] Reportedly, the government promised that "the personal information collected [would] be only used for the purpose of epidemiological investigation and [would] be automatically deleted after a few weeks."[59] The UN Special Rapporteur on the Right to Privacy concluded that in most instances, the Korean government "sought to rectify" measures it realized as privacy-intrusive.[60]

C. Legal Basis for Surveillance

Starting with the authoritarian governments of the twentieth century, the South Korean government has used the National Security Act (NSA) as the legal basis for its surveillance. The NSA was enacted in 1948 with the purpose of preventing anti-State acts from threatening the security of South Korea.[61] In fact, the law was a response to threats from communist Democratic People's Republic of Korea (North Korea).[62] However, the South Korean government has tended to expand the scope of the statute

---

[53] *Id.*
[54] Myungji Yang, *Behind South Korea's Success in Containing Covid-19: Surveillance Technology Infrastructures*, ITEMS (Jan. 21, 2021), https://items.ssrc.org/covid-19-and-the-social-sciences/covid-19-in-east-asia/behind-south-koreas-success-in-containing-covid-19-surveillance-technology-infrastructures/.
[55] *Id.*
[56] Jung Won Sonn, *supra* note 59.
[57] Myungji Yang, *supra* note 61.
[58] *Id.*
[59] *Id.*
[60] Visit to the Republic of Korea, Report of the Special Rapporteur on the right to privacy, Joseph Cannataci, 50 U.N. Doc. A/HRC/46/37/Add.6 (2022).
[61] Diane B. Kraft, *South Korea's National Security Law: A Tool of Oppression in an Insecure World*, 24 WIS. INT'L L.J. 627 (2006), https://uknowledge.uky.edu/cgi/viewcontent.cgi?article=1494&context=law_facpub.
[62] Kraft, *supra* note 61*; see also* GUKGA BOAHN BEOB [National Security Act] ART. 7 (S. KOR.)

beyond its original remit to silence domestic opposition, particularly in the mid- to late-twentieth century.[63]

The NSA's most controversial provision is Article 7, which 7 has been criticized by international observers for enabling punishment of persons "praising or sympathizing with an anti-State group."[64] Specifically, it states that persons who "'praise, encourage, disseminate or cooperate' with an anti-State group will be imprisoned up to seven years, while anyone who organizes or joins a group that intends to do any of those acts will receive a minimum of one year in prison."[65] Additionally, a minimum of two years imprisonment is imposed on those who "create or spread false information which may disturb national order."[66]

Article 7 has frequently been used as a legal basis to imprison people exercising their right to freedom of expression. For example, following the economic crisis of 1997-1998, the NSA was used against students and workers demonstrating against unemployment.[67] Despite the democratization of the South Korean government, the controversial NSA provisions remain largely untouched,[68] and there has not been much movement to limit its scope. The statute retains strong support for fear that "abolishing the law would compromise national security by leaving South Korea defenseless against North Korea."[69]

Finally, it must be noted that Korea has enacted several statutes that protect an individual's personal data from surveillance. The Protection of Communications Secrets Act (PCSA) was enacted in 1993 to protect the private communications and conversations of individuals.[70] The amended PCSA, in general, prohibits the interception and wiretapping of these communications without the issuance of a warrant.[71] In 2011, Parliament enacted the Personal Information Protection Act (PIPA) as a comprehensive data protection legislation after a series of laws enacted prior to regulating the processing of personal information by public and private institutions proved to be ineffective.[72] PIPA is known for being strictly enforced.[73] PIPA aims to

---

[63] *Id.*
[64] Kraft, *supra* note 61at 629; *see also* Gukga boahn beob [National Security Act] Art. 7 (S. Kor.).
[65] *Id.*
[66] *Id.*
[67] Statement by Amnesty International, *Republic Korea (South Korea): Concerns Relating to Freedom of Expression and Opinion*, Amnesty International (Jun. 1995), https://www.amnesty.org/es/wp-content/uploads/2021/06/asa250121995en.pdf.
[68] *See South Korea: Revise Intelligence Act Amendments*, Human Rights Watch (Dec. 2020), https://www.hrw.org/news/2020/12/22/south-korea-revise-intelligence-act-amendments.
[69] Kraft, *supra* note 61, at 636.
[70] *See generally* Protection of Communications Secrets Act (PCSA) (S. Kor.).
[71] *See* Cho hee Bae et al., *A Study on the Improving Information Investigation Techniques to guarantee Internet Safety and Personal Privacy*, J. Internet Comput. Serv. 79-88, 80 (2023), https://koreascience.kr/article/JAKO202319859473322.pdf.
[72] Dong Hyeong Kim and Do Hyun Park, *Automated decision-making in South Korea: a critical review of the revised Personal Information Protection Act*, Humanities & Social Sciences Communications 2, 4 (2024), https://doi.org/10.1057/s41599-024-03470-y.
[73] Peter Oladimeji, *South Korea data protection law (PIPA): Everything you need to know*, Didomi Blog (May 3, 2023), didomi.io/blog/south-korea-pipa-everything-you-need-to-know.

uphold the constitutional right to self-determination and the provisions provide oversight of government entities attempting to collect personal information of citizens and legal counters to narrow the interpretations of statutes like NSA.[74] For the purpose of this Article, these statutes are noteworthy as legal reforms by the Korean government in an effort to move away from unlimited surveillance of the population.

III. Reflections on the South Korean Case Study and the ALC in Pakistan

There are a number of parallels between Pakistan's current surveillance practices and the history of State surveillance in South Korea. Notably, both countries face the recent issue of the public release of private conversations involving the wives of the former president or prime minister as well as challenges to accountability for government malfeasance. Some of the parallels between the obstacles faced in Pakistan and those described in the South Korean case study in this regard suggest significant insights that are explored below. The scandal generated by the Audio Leaks Case has highlighted several challenges that Pakistan must address to make similar progress in curbing the its abusive surveillance practices and policies, namely, (a) overly broad laws authorizing or enabling virtually unlimited surveillance powers; (b) government agencies and other State actors exercising nearly unlimited surveillance powers with little to no effective oversight, judicial or otherwise; (b) the nonexistence of data protection laws; and (c) the susceptibility of ICT companies to surveillance and data requests by State actors.

A. Government Agencies' Power of Surveillance

Both South Korea and Pakistan have agencies with broad statutory authority to conduct intrusive surveillance. In March 2024, the Pakistan Telecommunication Authority (PTA), in response to the High Court's inquiry into the role of the government in the ALC, asserted its national security authority to intercept calls by telecom operators.[75] This takes place through PTA's own licensing clauses which permit the State to suspend or modify telecommunication systems and licenses over the preference of any licensee upon a broad declaration of emergency.[76] Furthermore, the Prevention of Electronic Crimes Act (PECA) grants surveillance powers to agencies within Pakistan.[77] There is no adequate oversight, and provisions grant powers to "law enforcement to seize digital devices and content."[78]

Similarly, 1980s legislation granted South Korea's intelligence agencies broad authority to collect and compile information regarding public safety against communists and plots to overthrow the government.[79] Despite transitioning to democratic rule, the Korean government has made no significant change to limit the scope of the power of

[74] Kim & Park, *supra* note72; *see also* Cho hee Bae et al., *supra* note 71.
[75] Qazi, *supra* note 1, at 6-8.
[76] *Id.*
[77] *Id.*
[78] Adrian Shahbaz et al., FREEDOM HOUSE, *supra* note 8.
[79] SAVADA & SHAW, SOUTH KOREA: A COUNTRY STUDY, *supra* note 12.

surveillance permitted by this statute.[80] However, the South Korean judicial system no longer permits the broad scope of this legislation to allow intrusive surveillance of civilians. As seen in Part I, South Korean officials who overreached in their surveillance of private citizens were subject to investigations and criminal convictions.[81]

B. Legislation

Both countries have legislation granting the government expansive legal authority to surveil citizens. The Pakistan Telecommunication Authority draws its power to surveil from the Pakistan Telecommunications (Reorganization) Act (2010), the Investigation of Fair Trial Act (2016), and the Telecom Act (1996).[82] In particular, Section 54 of the Telecommunications (Reorganization) Act grants the federal government the power to intercept conversations or to trace those conversations through any telecommunication system.[83] The Investigation of Fair Trial Act permits the interception of and direct access to all information upon the issuance of a warrant by a High Court judge.[84] There is also the Prevention of Electronic Crimes Act (PECA) which "grants powers to law enforcement to seize digital devices and content." [85] PECA, which penalizes acts of cyberterrorism, hate speech, defamation, and the dissemination of false information, has been widely abused and lacks proper oversight.[86] Such broad surveillance powers have resulted in allegations of intelligence agencies monitoring human rights defenders, journalists, politicians, and other dissidents or opponents of the current ruling political party.[87] With respect to the ALC, there has been no identified source linked to Bibi's and Saqib's released conversations; however, there is a widespread understanding that intelligence agencies had to have been involved.[88] In court, government agencies have denied any liability by citing to the aforementioned laws as the legal basis for collecting information from telecommunication companies.[89]

Similarly, the Korean National Security Act (NSA) was passed in the mid-twentieth century in order to punish "those praising or sympathizing with an anti-State group."[90] But the Act has been most often used to imprison people who exercised their right to freedom of expression in the twentieth century.[91] Significantly, although other political and judicial limitations have evolved, the South Korean government has not reformed

---

[80] *South Korea: Revise Intelligence Act Amendments*, Human Rights Watch, *supra* note 68; Statement by Amnesty International, *supra* note 67.
[81] *See*, e.g., *Jail sentence demanded for Lee's aide in illegal surveillance scandal*, *supra* note42*; see also* Republic of Korea 2020 Human Rights Report, U.S. Department of State, *supra* note 46.
[82] *Audio Leaks Case Fact File, supra* note 6.
[83] Pakistan: Freedom on the Net 2024 Country Report, Freedom House, https://freedomhouse.org/country/pakistan/freedom-net/2024.
[84] Qazi, *supra* note 1, at 8-10.
[85] Pakistan: Freedom on the Net 2024 Country Report, Freedom House, *supra* note 83.
[86] Pakistan: Freedom on the Net 2024 Country Report, Freedom House, *supra* note 83.
[87] Human Rights Committee, Concluding observations on the second periodic report of Pakistan, 44 CCPR/C/PAK/CO/2 (Dec. 2, 2024).
[88] Qazi, *supra* note 1, at 19-20, 24, 27.
[89] *Id.*
[90] Kraft, *supra* note 61*; see also* Gukga boahn beob [National Security Act] Art. 7 (S. Kor.).
[91] Kraft, *supra* note 61.

the statute to limit its broad scope; this despite human rights organizations criticizing how the Act violates international human rights norms.[92]

A key difference between the two case studies relates to data protection laws, emphasizing their importance. While South Korea has enacted a robust data protection legal framework, in part to counteract widespread abuse of surveillance powers, Pakistan has no stand-alone data protection legislation.[93] Despite some efforts to adopt such a law, there is currently no legislation in Pakistan that shields personal data from either private or government entities.

C. Role of Government Requests to Private Companies

Companies in both States are susceptible to government requests for users' private information. While it has not been ascertained yet as to how the audio leaks that were the subject of litigation occurred, the government's position was that user devices could have been hacked or accessed by a third party, and that it was not the result of "lawful" interception.[94] The position taken by telecom operators in the ALC was that there are several laws and regulations that require the disclosure of user data, in particular their licenses issued by the PTA, due to which they are obligated to comply.[95] Corporate telecom operators cited the same legal authorities as the PTA, specifically provisions that authorize government agencies to collect information from private companies, which is obligated through PTA's licensure requirement.

Similarly, South Korea permits government agencies to collect information from private companies through warrants and other legal government requests.[96] Former President Park Geun-hye attempted to use this opportunity to monitor private messages sent through Kakao Talk in order to crack down on messages deemed as critical of her presidency.[97] As mentioned above, an ICT company's susceptibility to the government's request to pry into its users' conversations led to the mass exodus of users, ultimately forcing the company to promise it would no longer respond to government requests for access to information.[98] Most importantly, it was an encouraging example of a company willing to push back on government data requests, and assume the possible legal consequences, in order to retain its customers' trust.

D. Concluding Observations

---

[92] *See South Korea: Revise Intelligence Act Amendments*, HUMAN RIGHTS WATCH, *supra* note 68; Statement by Amnesty International, *supra* note 67.
[93] *See* Sahar Iqbal, Data Privacy and Protection in Pakistan, International Bar Association (Jul. 24, 2023), ibanet.org/data-privacy-and-protection-in-Pakistan.
[94] *Supreme Court Halts Islamabad High Court Proceedings In Audio Leeks Case*, THE EXPRESS TRIBUNE (Aug. 19, 2024), https://tribune.com.pk/story/2489238/supreme-court-halts-islamabad-high-court-proceedings-in-audio-leak-case; Qazi, supra note 1, at 20.
[95] *Id.*
[96] *See*, e.g. Cho hee Bae et al., *supra* note 71; *see also* Kim & Park, *supra* note 72.
[97] *Why South Koreans are fleeing the country's biggest social network*, *supra* note 48.
[98] *Kakao Talk says 'no' to South Korean government demands*, *supra* note 52.

The foregoing makes clear a number of the similarities between the South Korean case study and the situation in Pakistan as exemplified by the ALC, in terms of government surveillance power and potential abuses of that power. The key question remaining is this: what are the *differences* between the two that might explain why government surveillance in South Korea has been scaled back, and is being held in check more effectively? In short, the experience of South Korea highlights the importance of global and domestic media attention, widespread popular mobilization, and the role of responsible ICT company conduct in combatting State overreach, among others. When these factors converge, the case study suggests, abusive surveillance policies and practices can be reined in and wrongdoers held accountable, at least to some extent.

South Korea is an example of how factors like domestic and global media coverage, along with public mobilization, can pressure governments to phase out abusive surveillance practices and even repeal repressive policies that violate constitutional and human rights. The press and public backlash to the Chun government's torture and killing of student activists Park Jong-chul in 1987; the negative coverage of government abuses in relation to South Korea hosting the 1988 Olympics; the scandals generated by the surveillance of political opponents during the administrations of Presidents Roh and Lee; and the huge outcry against President Park for spying on the families of the victims of the Sewol Ferry tragedy, as well as her political opponents, leading to her impeachment in 2016; these key moments in South Korea's history all reflect the way in which democratic forces can positively influence public policies on State surveillance and respect for privacy rights.

In addition, even where government agencies have broad surveillance powers authorized by statute, these positive forces can motivate ICT companies to "do the right thing," as Kakao Talk did in response to President Park's unlawful surveillance of its messaging app and network. Another key feature of the South Korean landscape that finds no direct corollary in Pakistan is the existence of a robust data protection legal framework that is strongly enforced; this acts to counterbalance at least some of the potential government overreach otherwise enabled by law. Indeed, ICT companies will be less susceptible to government surveillance and data requests when those powers are curbed by law in line with constitutional and human rights norms. Such legal reform in turn can be enabled by international media and diplomatic pressure, which dovetail with domestic public backlash to positive change—a dynamic that altered the practice of State surveillance in South Korea.

It should be noted that surveillance by the South Korean authorities remains ongoing despite the positive evolution of public policies over the past several decades. Surveillance is still being used against citizens to silence political opponents and dissidents. However, the South Korean media and legal system continue to push back against the State's overreach, fueled by the public's decreased tolerance of abusive practices for the historical reason discussed. And as technological advancements have made it faster and easier for South Korean citizens to access information, it has become harder for government officials to use surveillance powers against the interests of the people.