DigitalRightsFoundation
"KNOW YOUR RIGHTS"

Impact and Legality of Surveillance

Introduction

This document has been prepared by the Digital Rights Foundation on the issue of the constitutionality and social impact of surveillance, particularly from a human rights perspective. This short policy brief states that the surveillance, by both state and private actors, can have a profound impact on the freedoms of a democratic society and if done without adequate safeguards, has the potential to have a chilling effect on democratic freedoms.

The Digital Rights Foundation (DRF) is a non-governmental organization, established in 2012, working on the intersection of human rights with technology, with a particular focus on freedom of expression, right to privacy and protections against gender-based violence in online spaces.

This document was published on October 14, 2020.

State of Privacy in Pakistan

The Constitution of the Islamic Republic of Pakistan enshrines the right to privacy as a fundamental right. Article 14(1) of the Constitution confirms that "[t]he dignity of man and, subject to law, the privacy of home, shall be inviolable."

As a fundamental constitutional right, the right to privacy is meant to take precedence over any other inconsistent provisions of domestic law. Article 8 of the Constitution provides that "[a]ny law, or any custom or usage having the force of law, in so far as it is inconsistent with the rights conferred [under the Constitution], shall, to the extent of such inconsistency, be void." Article 8 (5), furthermore, states that "[t]he rights conferred by this Chapter shall not be suspended except as expressly provided by the Constitution."

Yet Pakistan's constitution also includes a wide-ranging exception to the primacy of fundamental rights.

Communication Surveillance

Pakistan's sizable population generates a huge amount of communications traffic. Approximately 79.65% of Pakistanis have a mobile phone subscription, according to the Pakistan Telecommunications Authority (PTA).[1] An estimated 35% of the population uses the internet. Fifty operational internet providers and six mobile operators serve this demand.

Social media platforms are widely used in Pakistan. The social network Facebook reportedly had approximately 36 million Pakistani users in 2019, 79% of which are purportedly male.[2] Twitter has approximately 1.8 million users (77.2% of which are men and 22.8% women).[3]

---

[1] "Telecom Indicators", https://www.pta.gov.pk/en/telecom-indicators.
[2] "Annual Report: 2019," Pakistan Telecommunications Authority, https://www.pta.gov.pk/assets/media/pta_ann_rep_2019_27032020.pdf.
[3] Simon Kemp, "Digital 2020: Pakistan." DataReportal. DataReportal – Global Digital Insights, February 18, 2020. https://datareportal.com/reports/digital-2020-pakistan.

Surveillance laws

A number of laws regulate communications surveillance in Pakistan.

The Investigation for Fair Trial Act (2013)

The IFTA was formalized in February of 2013 to '*to provide investigation for collection of evidence by means of modern techniques and devices to prevent and effectively deal with scheduled offences and to regulate the powers of the law enforcement and intelligence agencies for matters connected therewith*' as per the document of the Act itself.
The law essentially legalized the use of technology to intercept and track devices and people, for the purpose of maintaining national security however it received much criticism[4] from human rights factions for the possibility of misuse or abuse of power against citizens of the country.

The Prevention of Electronic Crimes Act (2016)

The PECA was a long time coming, several versions of the Bill had been presented to the national assembly and senate. The Bill had four major iterations, an April 2015 version, a September 2015 version, an April 2016 version and the final version passed in August 2016. Much ado was made of the fact that around 50 amendments were incorporated, however these amendments still left some of the major criticisms unaddressed.
The Act contains 28 offences including those penalising cyber stalking, harassment, hate speech and electronic fraud as well as provisions requiring service providers to retain traffic data (s.32) for a minimum period of a year unless the Authority (the FIA) specifies a different duration.
Beyond the rhetoric, a deeper analysis of PECA and its accompanying implementation structures reveals an ineptitude and unwillingness on part of the government to make online spaces safer. In fact, the Act has given ample leeway to the government to silence dissent and threaten opposition parties. Many of the fears put forward by digital rights activists were brought to fruition as there have

[4] "Listening in," *Dawn*, September 7, 2012, https://www.dawn.com/news/747592/listening-in.

been a worrying number of arrests and detentions of political opposition parties and their social media wings. Journalists have been questioned and arrested for allegedly "anti-state" comments online. Furthermore, criminalization of defamation via s. 20 (offences against the dignity of a natural person) has curtailed to a great extent the freedom of speech of the country's citizens. Since the passage of the law, section 20 has been used against journalists, activists and women speaking out against harassment and violence.

The Monitoring and Reconciliation of Telephony Traffic Regulations (2010)

In addition to the acts listed above, section 4 of the Monitoring and Reconciliation of Telephony Traffic Regulations (2010) requires each long distance and international service provider to establish a system that allows for real-time monitoring and recording of traffic on its networks.

Data retention

Under certain legal provisions, Pakistani providers are required to retain communications data as a condition of their operating license. Since 2004, network providers have been required to comply with requests for interception and access to network data as a standard condition of the PTA's award of operating licenses to phone companies.

The 2002 Electronic Transaction Ordinance (ETO) in sections 5 and 6 impose data retention requirements:

> "The requirement under any law that certain document, record, information, communication or transaction be retained shall be deemed satisfied by retaining it in electronic form if:
> (a) the contents of the document, record, information, communication or transaction remain accessible so as to be usable for subsequent reference;
> (b) the contents and form of the document, record, information, communication or transaction are as originally generated, sent or received, or can be demonstrated to represent accurately the

> contents and form in which it was originally generated, sent or received; and
> (c) such document, record, information, communication or transaction, if any, as enables the identification of the origin and destination of document, record, information, communication or transaction and the date and time when it was generated, sent or received, is retained."

The Prevention of Electronic Crimes Act (PECA) 2016 s. 32 states:

> "A service provider shall, within its existing or required technical capability, retain its specified traffic data for a minimum period of one year or such period as the Authority may notify from time to time and, subject to production of a warrant issued by the court, provide that data to the investigation agency or the authorized officer whenever so required."

Pakistan Telecommunication (Re-Organization) Act, 1996

The 1996 Act allows for interception of calls under section 54(1): "in the interest of national security or in the apprehension of any offence, the Federal Government may authorize any person or persons to intercept calls and messages or to trace calls through any telecommunication system". The the landmark case of *Benazir Bhutto v Federation of Pakistan and Others*, PLD 1998 SC 388 where it was declared that:

> "The inviolability of privacy is directly linked to the dignity of man. If a man is to preserve his dignity, if he is to live with honour and reputation, his privacy whether in the home or outside the home has to be saved from invasion and protected from illegal intrusion. The right conferred under Article 14 is not to any premises, home or office, but to the person, the man/woman wherever he/she may be."[5]

[5] Benazir Bhutto v Federation of Pakistan and Others, PLD 1998 SC 621.

This was in particular to address wiretapping by the Government and was declared unlawful, unless permission was sought and granted from the Supreme Court.

The Anti-Terrorism Act, 1997

The ATA was one of the first legislation that severely restricted the right to privacy. The controversial section 10[6] of the ATA, which initially allowed for broad powers of enter and search, was deemed unconstitutional by the Supreme Court in Mehram Ali vs. Federation Pakistan, PLD 1998 SC 1445:

> "Section 10 of the Anti-Terrorism Act, 1997 empowers an officer of the police, armed forces or civil armed forces on his being satisfied that there are reasonable grounds for suspecting that a person has in his possession some written material or recording in contravention of section 8, he may enter and search the premises where it is suspected that the material or recording is situated and may take possession of the same. This is directly in conflict with Article 14 of the Constitution, which confers a fundamental right as to the dignity of man by, inter alia, laying down that the dignity of man and, subject to law, the privacy of home shall be inviolable. No doubt, that the above right of privacy is subject to law but such law is supposed to be reasonable and in conformity with the constitutional mandate".

The Supreme Court's objections were taken into account and incorporated into the law through the 1998 Anti-Terrorism (Amendment) Ordinance.

Surveillance capabilities

[6] Section 10: Power to enter or search.- If any officer of the police, armed forces or civil armed forces is satisfied that there are reasonable grounds for suspecting that a person has possession of written material or a recording in contravention of section 8 he may enter and search the premises where it is suspected the material or recording is situated and take possession of the same; [Provided that the concerned, officer first record in writing his reasons and serve a copy thereof either on the person or on the premises.]

IMSI Catchers

Such equipment includes IMSI Catchers. IMSI Catchers are monitoring devices that transmit a strong wireless signal, which work to entice nearby phones to connect to the IMSI catcher, rather than mobile phone towers. While these devices are used to 'target' a particular individual's device by, for example, being aimed at his or her workplace they work by identifying all phones in the vicinity of the IMSI Catcher's operations. This means they could be used to identify unknown persons attending demonstrations and other gatherings because as many mobile phones as the system can accommodate will connect to the IMSI catcher and transmit it information about the mobile phone user, including the location of a target to within one metre.
Law enforcement agencies across Pakistan widely use mobile monitoring equipment for identification and/or interception. The Pakistani government has imported many tactical communications surveillance technologies from Europe. In 2010, the German government granted German companies export licenses valued at EUR 3.9 million to export "monitoring technology and spyware software" to Pakistan, according to Privacy International. Between 2012 and 2014, Swiss companies were granted licenses to export dual-use communications surveillance technology to Pakistan. The total value of the three exports based on the category provided was over CHF 1 million according to records obtained by Privacy International.

Intrusion malware

In 2014, someone hacked into the servers of FinFisher, the notorious surveillance software maker, which was reported to have two command and control servers inside Pakistan last year. The hackers got hold of whatever they could find on the server and leaked it as a torrent. The 40Gb torrent contains the entire FinFisher support portal including the correspondence between customers and the company staff. It also contains all the software that the company sells as well as the accompanying documentation and release material.
FinFisher is a company that sells a host of surveillance and monitoring software to government departments. The primary software, FinSpy, is used to remotely access

and control the computers or mobile phones belonging to the people being spied on.

A probe[7] by DRF looked into the situation back in 2014 after a University of Toronto based research group called Citizen Lab released a report[8] last year identifying two FinFisher command and control servers on the PTCL network.

Lawful interception on communications networks

Pakistan has a thriving communications surveillance industry that has developed to meet the growing demand for increased levels of surveillance. Pakistani companies such as the Center for Advanced Research in Engineering and the National Radio Telecommunication Corporation of Pakistan have all developed network surveillance tools, partly in collaboration with the military. Other companies provide both interception technologies as well as facilities to monitor and analyse transmitted data.

Packet Inspection

The same technologies that the Pakistani government uses for censorship are also used for surveillance. Censorship of online content is widespread and justified as a means to prevent the sharing of pornographic, obscene, and blasphemous material in the Islamic republic.

The Pakistani government has purchased a number of 'packet inspection' technologies. Pakistan Telecommunications Ltd (PTCL), Pakistan's largest telecommunications company that also operates the Pakistan Internet Exchange has proxies in place to do "deep packet inspection" of internet traffic.

[7] "Pakistan is a FinFisher customer, leak confirms," *Digital Rights Foundation*, https://digitalrightsfoundation.pk/pakistan-is-a-finfisher-customer-leak-confirms/.
[8] "For their Eyes Only", Citizen Lab, 2014, https://citizenlab.ca/storage/finfisher/final/fortheireyesonly.pdf.

In late October 2019, Pakistan's plan to engage the firm Sandvine Corporation, which is notorious for its Internet surveillance technologies, resurfaced with the publishing of a report highlighting details of the contract signed over the matter.[9]

The issue has been in the press since May 2019, when the government first announced plans for monitoring the country's internet traffic.[10]

Habeas Data/Subject access requests

Pakistan does not have any legislation explicitly allowing an individual to request data about themselves. However, it may be possible to request this information under Freedom of Information legislation.

Freedom of Information (FOI)

The Constitution of Pakistan grants the public the right to information via Article 19A, which states:

> "Every citizen shall have the right to have access to information in all matters of public importance subject to regulation and reasonable restrictions imposed by law."

There are several Acts at the provincial level that have built on this constitutional right, but since the passage of these laws, which have been on the surface considered robust in nature, the implementation of information requests by various commissions and the wide interpretation given to exceptions has rendered many of these laws toothless.[11]

---

[9] "Govt working with controversial firm to monitor internet traffic: report", Dawn, October 25, 2019, https://www.dawn.com/news/1512784.
[10] Luavut Zahid, "In dire straits: Pakistan's web monitoring", *MIT Technology Review*, February 6, 2020, http://www.technologyreview.pk/in-dire-straits-pakistans-web-monitoring/.
[11] "Status of Right to Information (RTI) in Pakistan 2020: June - September 2020," Centre for Peace and Development Initiatives (CPDI), http://www.cpdi-pakistan.org/wp-content/uploads/2020/09/Status-of-RTI-in-Pakistan-2020.pdf.

Data Protection Legislation Status

In July 2018, the Ministry of Information Technology and Telecommunication (MoITT) presented a draft data protection bill for consultation. A second version of the Bill was released in October of the same year and then the third version was published by the Ministry in April of 2020. Comments and suggestions were provided by the civil society at large and also by us at the Digital Rights Foundation that can be accessed here.
The legislative process is still on-going at the time of publication of this document.

The Right to Privacy in International and Regional Treaties

Universal Declaration of Human Rights, Article 12 (10 December 1948)

> "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

European Convention for the Protection of Human Rights and Fundamental Freedoms, Article 8: Right to Respect for Private and Family Life (4 November 1950)

> "1. Everyone has the right to respect for his private and family life, his home and his correspondence.
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

Pakistan is signatory to at least three Conventions with privacy implications:

1. International Covenant on Civil and Political Rights (ICCPR)
2. Cairo Declaration on Human Rights in Islam (CDHRI)
3. Convention on the Rights of the Child (CRC)

This is a non-exhaustive list, with many more additions such as the Arab Charter on Human Rights and the Charter of Fundamental Human Rights of the EU etc that all contain passages which recognize without doubt the sanctity of the right to privacy of the individual.

International Covenant on Civil and Political Rights, Article 17 (16 December 1966)

> "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
> 2. Everyone has the right to the protection of the law against such interference or attacks."

Human Rights Council, Fortieth Session, February and March 2019, 'Right to Privacy', Report by the Special Rapporteur on the right to privacy

The Council states that the right to privacy is "integral to discussions about autonomy" and must be upheld in accordance with democractic principles.

Principles of Legality, Necessity, Proportionality and Adequate Safeguards

We have noted below a brief discussion of persuasive precedents and opinions on the principles surrounding surveillance and the right to privacy:

(A) The Principle of Legality

U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/RES/73/179 (17 December 2018)

> "Noting in particular that surveillance of digital communications must be consistent with international human rights obligations and must be conducted on the basis of a legal framework, which must be publicly accessible, clear, precise, comprehensive and non-discriminatory, and that any interference with the right to privacy must not be arbitrary or unlawful, bearing in mind what is reasonable with regard to the pursuance of legitimate aims, and recalling that States that are parties to the International Covenant on Civil and Political Rights must take the necessary steps to adopt laws or other measures as may be necessary to give effect to the rights recognized in the Covenant,"

(B) The Principle of Necessity

Szabó and Vissy v. Hungary, App. No. 37138/14, European Court of Human Rights, Judgment (12 January 2016)

> "However, given the particular character of the interference in question and the potential of cutting edge surveillance technologies to invade citizens' privacy, the Court considers that the requirement "necessary in a democratic society" must be interpreted in this context as requiring "strict necessity" in two aspects. A measure of secret surveillance can be found as being in compliance with the Convention only if it is strictly necessary, as a general consideration, for the safeguarding the democratic institutions and, moreover, if it is strictly

necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation. In the Court's view, any measure of secret surveillance which does not correspond to these criteria will be prone to abuse by the authorities with formidable technologies at their disposal. The Court notes that both the Court of Justice of the European Union and the United Nations Special Rapporteur require secret surveillance measures to answer to strict necessity – an approach it considers convenient to endorse."

(C) The Principle of Proportionality

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, U.N. Doc. A/69/397 (23 September 2014)

"51. It is incumbent upon States to demonstrate that any interference with the right to privacy under article 17 of the Covenant is a necessary means to achieving a legitimate aim. This requires that there must be a rational connection between the means employed and the aim sought to be achieved. It also requires that the measure chosen be "the least intrusive instrument among those which might achieve the desired result". The related principle of proportionality involves balancing the extent of the intrusion into Internet privacy rights against the specific benefit accruing to investigations undertaken by a public authority in the public interest. However, there are limits to the extent of permissible interference with a Covenant right. As the Human Rights Committee has emphasized, "in no case may the restrictions be applied or invoked in a manner that would impair the essence of a Covenant
right". In the context of covert surveillance, the Committee has therefore stressed that any decision to allow interference with communications must be taken by the authority designated by law "on a case by-case basis". The proportionality of any interference with the right to privacy should therefore be judged on the particular circumstances of the individual case."

(D) The Principle of Adequate Safeguards

U.N. Human Rights, General Comment No. 16: Article 17 (Right to Privacy), U.N. Doc. HRI/GEN/1/Rev.1 at 21 (8 April 1988)

> "10. … Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant."

Rights-Based Approach to Surveillance

Excerpt from the Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37 (30 June 2014):

"The secret nature of specific surveillance powers brings with it a greater risk of arbitrary exercise of discretion which, in turn, demands greater precision in the rule governing the exercise of discretion, and additional oversight."

In 2013, a coalition of civil society organisations developed "International Principles on the Application of Human Rights to Communications Surveillance" highlighting a human rights approach to surveillance.[12] These principles, though not adopted by any state party, the principles highlight the ways in which international human rights law applies to surveillance practices. The principles are 1) legality: "any imitation to the right to privacy must be prescribed by law"; 2) legitimate aim: "laws should only permit communications surveillance by specified State authorities to achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society. Any measure must not be applied in a manner which discriminates on the basis of race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status."; 3) necessity: "strictly and demonstrably necessary to achieve a legitimate aim"; 4) adequacy: "must be appropriate to fulfil the specific legitimate aim identified"; 5) proportionality: "should be regarded as a highly intrusive act that interferes with the rights to privacy and freedom of opinion and expression, threatening the foundations of a democratic society"; 6) competent judicial authority: "determinations related to communications surveillance must be made by a competent judicial authority that is impartial and independent"; 7) due process: "that lawful procedures that govern any interference with human rights are properly enumerated in law, consistently practiced, and available to the general public"; 8) user notification: "individuals should be notified of a decision authorising communications surveillance with enough time and information to enable them to

[12] "July 2013 Version: International Principles on the Application of Human Rights to Communications Surveillance", Necessary & Proportionate, https://necessaryandproportionate.org/july-2013-principles/.

appeal the decision"; 9) transparency: "about the use and scope of communications surveillance techniques and powers"; 10) public oversight: "establish independent oversight mechanisms to ensure transparency and accountability of communications surveillance"; 11) integrity of communications and systems: "States should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems, or to collect or retain particular information purely for State surveillance purposes"; 12) safeguards for international cooperation: "States may not use mutual legal assistance processes and foreign requests for protected information to circumvent domestic legal restrictions on communications surveillance"; 13) safeguards against illegitimate access: "enact legislation criminalising illegal communications surveillance by public or private actors".[13]

U.N. General Assembly Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/RES/73/179 (17 December 2018)

> "Noting in particular that surveillance of digital communications must be consistent with international human rights obligations and must be conducted on the basis of a legal framework, which must be publicly accessible, clear, precise, comprehensive and non-discriminatory, and that any interference with the right to privacy must not be arbitrary or unlawful, bearing in mind what is reasonable with regard to the pursuance of legitimate aims, and recalling that States that are parties to the International Covenant on Civil and Political Rights must take the necessary steps to adopt laws or other measures as may be necessary to give effect to the rights recognized in the Covenant."

[13] "Necessary & Proportionate: International Principles on the Application of Human Rights to Communications Surveillance", May 2014, https://www.ohchr.org/documents/issues/privacy/electronicfrontierfoundation.pdf.

Types of Surveillance

(1) Mass Surveillance

Mass surveillance often involves monitoring, interception, collection, analysis, use, preservation and retention of, interference with, or access to data, communications content and information about communications, or "communications metadata", at a mass scale as opposed to targeted and tailored surveillance practices.

One of the most prominent examples of mass surveillance is the National Security Agency (NSA) dragnet mass surveillance program that collected telephone records of US citizens. The program was exposed by Edward Snowden and has been declared as unconstitutional by the U.S. Court of Appeals for the Ninth Circuit.

United States v. Moalin, U.S. Court of Appeals for the Ninth Circuit

It was held that the government may have violated the Fourth Amendment and did violate the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. 1861, when it collected the telephony metadata of millions of Americans, including at least one of the defendants, but suppression was not warranted in this case because the metadata collection did not taint the evidence introduced at trial. The court's review of the classified record confirmed that the metadata did not and was not necessary to support the probable cause showing for the FISA warrant application.

(2) Targeted Surveillance

Targeted surveillance (or targeted interception) is a form of surveillance, such as wiretapping, that is directed towards specific persons of interest, and is distinguishable from mass surveillance (or bulk interception). Despite being less expensive than mass surveillance, targeted surveillance can only be permissible when it is prescribed by law and pursues a legitimate aim. (Weber and Saravia v. Germany - no. 54934/00, 2006).

Strategic monitoring of telecommunications.
Safeguards regarding media freedom

Weber and Saravia v. Germany - no. 54934/00
Decision 29.6.2006

Facts: In 1994 the Act of 13 August 1968 on Restrictions on the Secrecy of Mail, Post and Telecommunications (Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses), also 6 called "the G 10 Act" (See Klass and Others v. Germany, judgment of 6 September 1978, Series A no. 28) was amended to accommodate the so-called strategic monitoring of telecommunications, that is, collecting information by intercepting telecommunications in order to identify and avert serious dangers facing the Federal Republic of Germany, such as an armed attack on its territory or the commission of international terrorist attacks and certain other serious offences. The changes notably concern the extension of the powers of the Federal Intelligence Service (Bundesnachrichtendienst) with regard to the recording of telecommunications in the course of strategic monitoring, as well as the use of personal data obtained thereby and their transmission to other authorities. The first applicant, a German national, is a freelance journalist; the second applicant, a Uruguayan national, took telephone messages for the first applicant and passed them on to her. In 1995 the applicants lodged a constitutional complaint with the Federal Constitutional Court challenging the new amendments.

Article 8 – Restating earlier case-law, the Court notes that the mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an interference with the exercise of the applicants' rights under Article 8, irrespective of any measures actually taken against them. The transmission of data to and their use by other authorities, which enlarges the group of persons with knowledge of the personal data intercepted, constitutes a further separate interference with the applicants' rights under Article 8.

As to whether these interferences are "in accordance with the law", the Court notes that the term "law" within the meaning of the Convention refers back to national law, including rules of public international law applicable in the State concerned; as regards allegations that a respondent State has violated international law by

breaching the territorial sovereignty of a foreign State, the Court requires proof in the form of concordant inferences that the authorities of the respondent State have acted extraterritorially in a manner that is inconsistent with the sovereignty of the foreign State and therefore contrary to international law. The impugned provisions of the amended G 10 Act authorise the monitoring of international wireless telecommunications, that is, telecommunications which are not effected via fixed telephone lines but, for example, via satellite or radio relay links, and the use of data thus obtained. Signals emitted from foreign countries are monitored by interception sites situated on German soil and the data collected are used in Germany. In the light of this, the Court finds that the applicants failed to provide proof in the form of concordant inferences that the German authorities, by enacting and applying strategic monitoring measures, have acted in a manner which interfered with the territorial sovereignty of foreign States as protected in public international law.

As to the statutory basis of the amended G 10 Act, the Court accepts the judgment of the Federal Constitutional court that it satisfies the Basic Law and finds no arbitrariness in its application. As to the quality of the law, firstly, its accessibility raises no problem; secondly, the Court concludes that the impugned provisions of the G 10 Act, seen in their legislative context, contained the minimum safeguards against arbitrary interference as defined in the Court's case-law and therefore gave citizens an adequate indication as to the circumstances in which and the conditions on which the public authorities were empowered to resort to monitoring measures, and the scope and manner of exercise of the authorities' discretion.

The "legitimate aims" pursued were to safeguard national security and/or to prevent crime. 7 As to whether the interferences were "necessary in a democratic society", the Court recognises that the national authorities enjoy a fairly wide margin of appreciation in choosing the means for protecting national security. Nevertheless, in view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there exist adequate and effective guarantees against abuse. As to strategic monitoring per se, although the amended G 10 Act broadens the range of subjects in respect of which it can be carried out, safeguards against abuse were spelled out in detail and the Federal

Constitutional Court in fact raised the threshold in respect of at least one crime; the Court is satisfied that there was an administrative procedure designed to ensure that measures were not ordered haphazardly, irregularly or without due and proper consideration.

As regards supervision and review of monitoring measures, the system of supervision was essentially the same as that found by the Court in its Klass and Others judgment not to violate the Convention; there is no reason to reach a different conclusion in the present case. As to the transmission of non-anonymous personal data obtained by the Federal Intelligence Service to the Federal Government, the Court accepts that transmission of personal – as opposed to anonymous – data might prove necessary. The additional safeguards introduced by the Federal Constitutional Court, namely that the personal data contained in the report to the Federal Government were marked and remain connected to the purposes which had justified their collection, are appropriate for the purpose of limiting the use of the information obtained to what is necessary to serve the purpose of strategic monitoring. As to the transmission of personal data to, among other authorities, the Offices for the Protection of the Constitution, the Court notes that the crimes for which this was possible were limited to certain designated serious criminal offences and that following the Federal Constitutional Court's judgment such transmission, which had to be recorded in minutes, was only possible if the suspicion that someone had committed such an offence was based on specific facts as opposed to mere factual indications; the safeguards against abuse, as thus strengthened by the Federal Constitutional Court, were adequate.

As to the destruction of personal data, an acceptable procedure for verifying whether the conditions were met was in place; moreover, the Federal Constitutional Court had ruled that data which were still needed for court proceedings could not be destroyed immediately and had extended the supervisory powers of the G 10 Commission to cover the entire process of using data up to and including their destruction.

Finally, as to the notification of persons whose communications had been monitored, this was to be done as soon as possible without jeopardising the purpose of the monitoring; rules contained in the judgment of the Federal

Constitutional Court prevented the duty of notification from being circumvented, save in cases where the data were destroyed within three months without ever having been used.

Manifestly ill-founded

Article 10 – The first applicant submitted that the amended G 10 Act prejudiced the work of journalists investigating issues targeted by surveillance measures. She could no longer guarantee that information she received in the course of her journalistic activities remained confidential. In the Court's view, the threat of surveillance constitutes an interference to her right, in her capacity as a journalist, to freedom of expression. The Court finds, on the reasons set out under Article 8, that this interference is prescribed by law and pursues a legitimate aim. As to necessity in a democratic society, the Court notes that strategic surveillance was not aimed at monitoring journalists; generally the authorities would know 8 only when examining the intercepted telecommunications, if at all, that a journalist's conversation had been monitored. Surveillance measures were, in particular, not directed at uncovering journalistic sources. The interference with freedom of expression by means of strategic monitoring cannot, therefore, be characterised as particularly serious. It is true that the impugned provisions of the amended G 10 Act did not contain special rules safeguarding the protection of freedom of the press and, in particular, the non-disclosure of sources, once the authorities had become aware that they had intercepted a journalist's conversation. However, the Court, having regard to its findings under Article 8, observes that the impugned provisions contained numerous safeguards to keep the interference with the secrecy of telecommunications – and therefore with the freedom of the press – within the limits of what was necessary to achieve the legitimate aims pursued. In particular, the safeguards which ensured that data obtained were used only to prevent certain serious criminal offences must also be considered adequate and effective for keeping the disclosure of journalistic sources to an unavoidable minimum.

(3) Amassing Social Media-based and Public Data

Other forms of surveillance is the collection of semi-private or publicly available information to surveil individuals and groups. In the age of social media and digitised transformations, so many users voluntarily share information with companies and public bodies in using their services. This information can often be used by the data collectors and third-parties to surveil citizens. For instance, in 2016 it was reported by the American Civil Liberties Union (ACLU) reported that Twitter, Facebook, and Instagram were providing user data access to a private company called Geofeedia which developed a social media monitoring product marketed to law enforcement as a tool to monitor activists and protesters.[14]

(4) Emerging Technologies and Surveillance

There are many types of emerging surveillance issues that are linked to technologies such as use of closed-circuit television (CCTV) cameras for urban policing, facial recognition technology (FRT) and applications such as those used for contact tracing during the Covid-19 pandemic. A critical appraisal of emerging surveillance technologies involves use of artificial intelligence (AI) and machine learning to combine data collection through surveillance with AI. This has led international groups such as the European Commission's High-Level Expert Group to issue Principles[15] and Ethics Guidelines[16] on the use of AI, particularly in relation to surveillance tech. Furthermore, the United States Special Rapporteur on freedom of opinion and expression, in 2019, for a moratorium on "the sale, transfer and use of surveillance technology until human rights-compliant regulatory frameworks are in place."[17]

---

[14] "Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color", ACLU, 2016, https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target.
[15] "Recommendation of the Council on Artificial Intelligence", OECD, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.
[16] "Ethics guidelines for trustworthy AI", EU, April 2019, https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.
[17] "UN expert calls for immediate moratorium on the sale, transfer and use of surveillance tools", https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24736.

Human Rights Council, Twenty Seventh Session, June 2014, 'The Right to Privacy in the Digital Age', Report of the Office of United Nations High Commissioner for Human Rights

It was noted that mass surveillance can impact rights in addition to the right to privacy such as freedom of expression and opinion, right to receive, seek and impart information, freedom to peaceful assembly and association, right to family life and right to health.

The Council stated that interception and collection of data about communication (meta data), as opposed to the contents of the communications, also constitutes an interference with privacy. "The aggregation of information commonly known as 'metadata' may give insight into an individual's behaviour, social relationships, private preferences, and identity that go beyond even that conveyed by accessing the content of a private communication."[18]

The overall sentiment, for those observing or participating in the digital spaces is that privacy is a foregone conclusion, owing to the vast number of intrusions via social media, targeted advertising, the ability to 'tap in' to dormant speakers and cameras on electronic gadgets. Hearing about instances like the Cambridge Analytica Scandal and its substantial impact on the American democratic machinery, or in our context, the NADRA breach resulting in CNIC information of thousands of Pakistani citizens being sold online for chump change instills the opposite of a sense of security in the people.

When this is aggregated by the writ of the law allowing for surveillance on its citizens, the compounded effect is that of residing in a glass house. The reasons for surrendering some freedoms to allow the State to provide us with the rest is what the earlier mentioned social contract theory talks of and indeed concerns such as national security are paramount. However the lack of checks and balances, a framework that details the need for and use of measures taken or the information collected or any other tools of accountability draws out the concerns of civil society and in particular digital rights actors.

[18] "Guide to International Law and Surveillance 2.0", Privacy International, February 2019, https://privacyinternational.org/sites/default/files/2019-04/Guide%20to%20International%20Law%20and%20Surveillance%202.0.pdf

DigitalRightsFoundation

"KNOW YOUR RIGHTS"

Legal Framework Exceeding Purpose

> *Governments are conducting surveillance by analyzing and exchanging ever greater quantities of information on their citizens, using data mining to233ols to identify individuals "of interest."*
> *A "digital tsunami" of data about individuals is produced by modern technologies. Companies are required in many jurisdictions to provide law enforcement and intelligence agencies with access to this data – and in some cases explicitly to retain data for longer than necessary for business purposes.*[19]

This excerpt from Ian Brown's paper on 'Social Media Surveillance', especially the ending pertains specifically in case of s. 32 of the Prevention of Electronic Crimes Act 2016 which details that a service provider shall retain traffic data for the minimum period of one year or as mandated by the Authority (FIA).

[19] Ian Brown, "Social Media Surveillance", The International Encyclopedia of Digital Communication and Society, First Edition, 2015, https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781118767771.wbiedcs122.

Encryption in Pakistan: An Attempt at Privacy

Through multiple notices since 2010 and then through it's notice on June 10 of this year, the Pakistan Telecommunication Authority stated that the use of VPNs (Virtual Private Networks) must be registered by the end of the month. This then received two extensions bringing the date to September 30th, 2020. For this notification, as with all others regarding encryption, no rationale was provided by PTA, neither was any framework laid down or indicated as to who will be collecting the data, where will it be held and will the Authority or the State be monitoring this usage or simply maintaining a record of the citizens, companies and organizations that employ VPN services while browsing the internet.
In Pakistan, where the Pakistan Telecommunications Authority (PTA) reported to a Senate committee that it had blocked more than 850,000 'objectionable' URLs since 2010, the use of VPNs is as innocuous as accessing websites that have either been blocked or do not offer their services in Pakistan--this includes streaming and educational services. This move serves to increase the feeling of vulnerability and visibility for the citizens wishing to remain anonymous whilst online.

McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995)

The Supreme Court of the United States held that The freedom to publish anonymously is protected by the First Amendment and "extends beyond the literary realm to the advocacy of political causes." It was established that "anonymity is a shield from the tyranny of the majority".

Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, U.N. Doc. A/HRC/39/29 (3 August 2018)

> "20. … Encryption and anonymity provide individuals and groups with a zone of privacy online where they can hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks (A/HRC/29/32). Encryption and anonymity tools are widely used around the world, including by human rights defenders, civil society, journalists, whistle-blowers and political dissidents facing persecution and harassment. Weakening them jeopardizes the privacy of all users

and exposes them to unlawful interferences not only by States, but also by non-State actors, including criminal networks.27 Such a widespread and indiscriminate impact is not compatible with the principle of proportionality (see A/HRC/29/32, para. 36)."

Social Impact of Surveillance

Illegal and illegitimate surveillance, by both states and private actors, has the impact of intrusions onto the private lives of citizens, not only violating their constitutional rights but also intrudes on the very personhood of those surveilled.

Surveillance particularly tends to exacerbate existing social hierarchies and systems of discrimination on the basis of race, ethnic identity, class, religion, gender identity, sexual orientation and disabilities. Surveillance of marginalised bodies and the impact that it can have is well documented in social science literature and has legal implications as it has disparate impact on certain populations, violating principles of non-discrimination and equality as enshrined in our constitution (Article 25).

Writing for the Harvard Law Review in 2013, Neil Richards states that surveillance has the impact of chilling the exercise of our civil liberties, "it can cause people not to experiment with new, controversial, or deviant ideas."[20] Furthermore, surveillance is often exercised as power by the watcher over the watched, as a form of control: "This disparity creates the risk of a variety of harms, such as discrimination, coercion, and the threat of selective enforcement, where critics of the government can be prosecuted or blackmailed for wrongdoing unrelated to the purpose of the surveillance."[21]

Surveillance and illegitimate intrusions into privacy impact the essential work that journalists, academics and activists do. Undue surveillance can lead to a chilling effect on those critical of state institutions and societal norms.

Human Rights Council, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", 2013, A/HRC/23/40

> "Undue interference with individuals' privacy can both directly and indirectly limit the free development and exchange of ideas. Restrictions of anonymity in communication, for example, have an

[20] Neil M. Richards, "The Dangers of Surveillance", Harvard Law Review, 2013, vol. 126, p. 1935, https://harvardlawreview.org/wp-content/uploads/pdfs/vol126_richards.pdf.
[21] Ibid.

evident chilling effect on victims of all forms of violence and abuse, who may be reluctant to report for fear of double victimization."

Public Interest and Surveillance

Big Brother Watch v. The United Kingdom, September 13, 2018, App nos. 58170/13, 62322/14 and 24960/15, European Court of Human Rights

The European Court of Human Rights found some aspects of the UK's mass surveillance regime to be in violation of the right to privacy and the right to freedom of expression under the European Convention on Human Rights (Convention). The case sought to challenge three different systems of mass surveillance adopted by the UK intelligence services: (1) the bulk interception of communications; (2) intelligence sharing with foreign governments; and (3) the obtaining of communications data from communications service providers. The Court found that a regime of bulk interception was not, in itself, incompatible with the European Convention on Human Rights. Nonetheless, it found the bulk interception regime in the UK to be in violation of the right to privacy and the right to freedom of expression due to, among other things, the lack of independent oversight over the entire process for selecting bearers for interception, identifying the selectors and search terms to be used to filter intercepted communications, and the selection of material to be examined by analysts. The Court also found the regime for obtaining communications data from communications service providers to be incompatible with the Convention because its use was not limited to combating "serious crime", it was not subject to prior review by a national authority, and it did not sufficiently protect journalists' confidential communications. The Court upheld the compatibility of the UK's intelligence sharing regime with the Convention.

Courts have held that surveillance, even if it seems the requirements of proportionality and legitimate aim, can be struck down on human rights grounds in the absence of adequate safeguards:

Dragojević v. Croatia, January 15, 2015, 68955/11, European Court of Human Rights

The Court found that the Croatian court's decision to authorize surveillance on Ante Dragojević's phone in a case involving allegations of possible drug trafficking

between Latin America and Europe via ocean carriers was unlawful under Article 8 of the European Convention on Human Rights (ECHR). Dragojević, a sailor, was subjected to secret surveillance for a period of 6 months. It was found that Croatia's domestic procedures for authorizing surveillance did not provide sufficient safeguards against potential abuse through surveillance. It was not sufficiently clear regarding the scope and manner of exercise of the discretion conferred on Croatia's public authorities, and it did not secure adequate safeguards against possible abuse.

Carpenter v. United States, 484 US 19 (2018)

In 2011, police officers arrested four men in connection with a series of robberies at RadioShack and T-Mobile stores in Michigan and Ohio, USA. One of these men provided a confession which included the cellphone numbers of some of his accomplices which the federal prosecutors then used in applying for cell records under the Stored Communications Act, 1994. Timothy Carpenter was one of the individuals whose number had been provided to law enforcement and whose records were obtained as a result. The material sought by prosecutors was "cell-site location information" or CSLI.
The United States Supreme Court held that obtaining cellular location data constitutes a search under the Fourth Amendment of the U.S. Constitution, and thus requires a warrant supported by probable cause. In a 5-4 decision, the Court expressed concern that cellphone records can provide "near perfect surveillance" and that the data is retained for many years and for all users, and held that an individual does have a "reasonable expectation of privacy" in respect of their cellphone location information. Accordingly, the Court ruled that the accessing of the individual's cellphone location data was an unconstitutional search and therefore a violation of the Fourth Amendment.