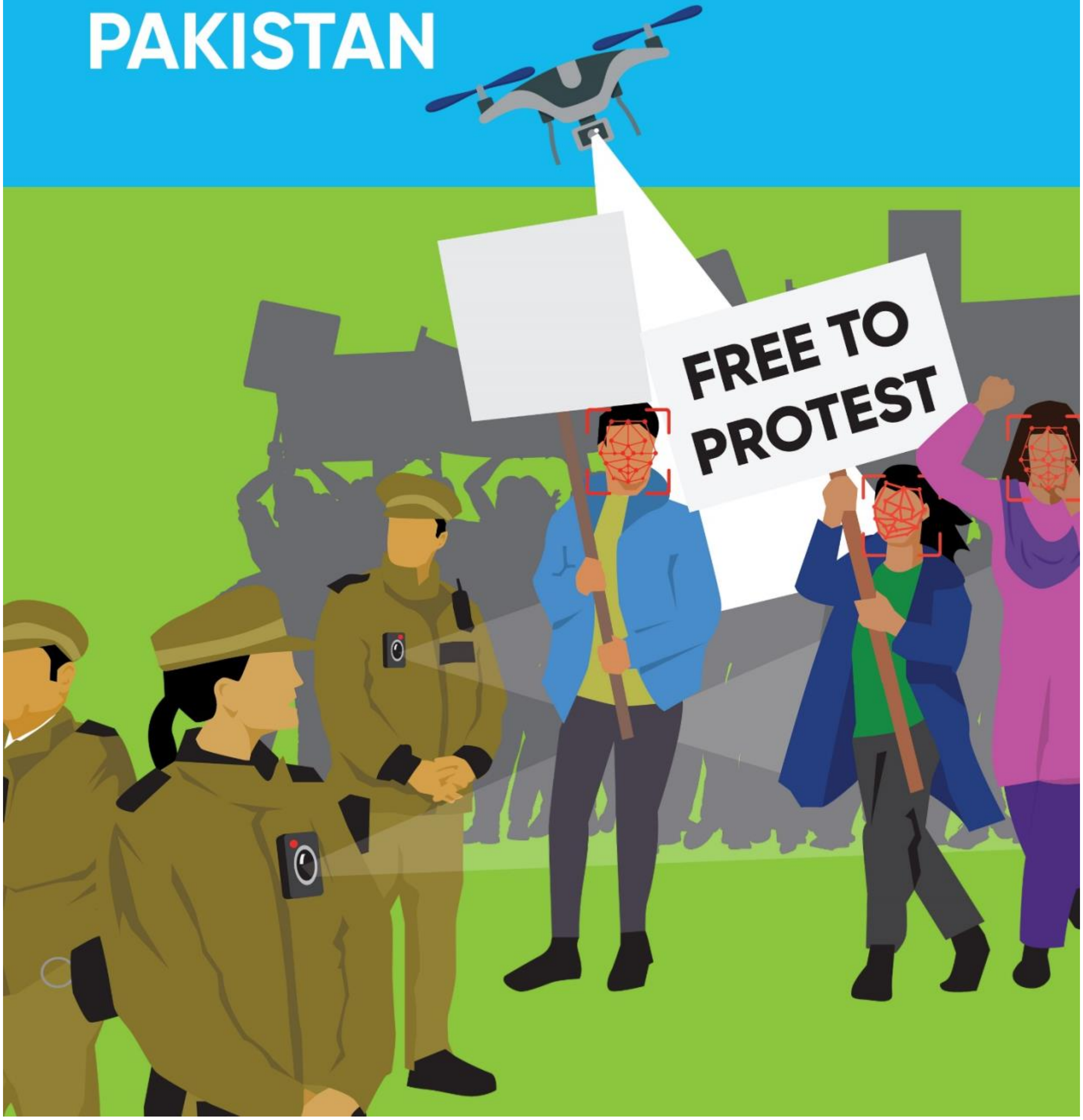
FREE TO PROTEST GUIDE PAKISTAN



Free to Protest Guide Pakistan

This Guide has been created by adapting the Free to Protest Guide UK according to the laws and policies of Pakistan, in collaboration with local activists and Privacy International.
It is not intended as a substitute to legal advice and serves only to lay out a set of information on and around protest safety.

What Does the Law Say?

The right to protest is recognized the world over as a basic democratic freedom. Pakistan, as a democratic nation, recognizes this right for its citizens.

Article 16 of the Constitution of the Islamic Republic of Pakistan, 1973 (as amended) grants every citizen the right, "*to assemble peacefully and without arms, subject to any reasonable restrictions imposed by law in the interest of public order*."

However, freedoms of assembly and association under Articles 16 and 17 of the Constitution of Pakistan are not unrestricted and the state may impose "reasonable restrictions" as per law in the interest of what it terms "public order." Under this exception, laws such as the Maintenance of Public Order Ordinance, 1960 have been used to curb public gatherings and arrest protestors. Further Section 144 of the Criminal Procedure Code (CrPC), 1973 has also been used to restrict gatherings of more than 5 people to prevent "obstruction, annoyance or injury to any person lawfully employed, or danger to human life, health or safety, or a disturbance of the public tranquillity, or a riot, of an affray."

Pakistan is also a signatory to multiple international human rights covenants and treaties and by definition is liable to uphold the principles and rules of those agreements.

Particularly of note is that Pakistan is a State Party to the 1966 International Covenant on Civil and Political Rights (ICCPR) and ratified the Covenant in 2010. Article 21 of this Covenant states that:

> *The right of peaceful assembly shall be recognized. No restrictions may be placed on the exercise of this right other than those imposed in conformity with the law, and which are necessary in a democratic society in the interests of*

> *national security or public safety, public order (order public), the protection of public health or morals or the protection of the rights and freedoms of others.*

This Guide has been created to facilitate the exercise of the right to freedom of association and assembly, and more specifically the right to protest and do so safely by mitigating the risks to one's privacy and data. We hope the following chapters help clarify some risks and mitigation measures for those citizens who choose to exercise their constitutional freedoms.

We are invested in having this be a living document that can evolve as the situation and pressures do as well, and to that end we look forward to receiving any feedback on improving and making relevant changes and additions to the Guide. For the same, please send in your communications at info@privacyinternational.org with the subject line "Pakistan protest guide".

Here are some **general tips** of what other activists are doing before and during attending protests:

1. Carry water for hydration. In case of tear gas deployment, flush out your eyes (start from the tear duct and wash outwards!).
2. Employ the 'buddy system', to help ensure no one is left behind in case of confusion or stampede if the police arrive and attempt to disperse the crowd or otherwise disrupt the protest.
3. Keep your phone fully charged and share location with a loved one before leaving for the protest.
4. Enable a passcode on your phone, disable any facial or fingerprint unlocks.
5. Do not bring devices that contain sensitive information with you to the protest
6. Wear a mask to protect yourself from dirt, pollutants and to also help obscure your face in case anyone is recording images or videos.
7. Document any injuries caused by police by taking pictures or videos.
8. Do not share images of fellow protestors on social media to avoid their presence being identified. You can use pictures with blurred or obscured faces.
9. Have an exit strategy defined for yourself and your companions.

Circumventing Internet or Network Shutdowns

What can be done in case of Internet shutdowns:

Disruption of Internet and mobile networks has unfortunately become a commonplace medium to disrupt protests. Not only do Internet shutdowns hamper vital human freedoms, but blocking communication can have serious consequences for protestors in case of panic or upheaval at a demonstration. In Pakistan, Internet shutdowns have been reportedly used to control mass gatherings[1] and protests.[2] The government often employs section 54(3) of the *Pakistan Telecommunications (Re-organization) Act, 1996* to shut down mobile networks. The sub-section states that upon proclamation of an emergency by the President the PTA may suspend or modify any licenses under the Act or cause suspension of operation, functions or services.

Here are some app-based options to lessen the impact of network blocking:

1. **FireChat** is an app that uses Bluetooth to exchange messages. It is available for both iOS and Android, with an effective range of 100m and 60m respectively.
2. **Briar** is a messaging app designed for activists, journalists, and anyone else who needs a safe, easy and robust way to communicate. It uses Bluetooth or WiFi to keep information flowing in a crisis. It is available on Android only.
3. **Bridgefy** is a messaging app allowing users to send encrypted messages through ad-hoc networks like peer-to-peer Wi-Fi and Bluetooth. It is available for both Android and iOS.

** NB: These apps have been suggested as a mitigation strategy and not a solution to illegal interception of messages or as a complete countermeasure to Internet disruption*

[1] Imran Asghar, “No mobile, internet service today,” The Express Tribune, March 23, 2022, https://tribune.com.pk/story/2349211/no-mobile-internet-service-today.
Muneeb Ahmad, “Mobile services to remain suspended in 52 cities on Muharram,” TechJuice, October 10, 2021, https://www.techjuice.pk/mobile-services-to-remain-suspended-in-52-cities-on-muharram/.

[2] Berhan Taye, “Pakistan shuts down the internet three times in one week,” Access Now, November 6, 2018, https://www.accessnow.org/pakistan-shutdowns-internet/.

What We Know So Far about the Surveillance Capabilities in Pakistan:

1. The Punjab Safe Cities Authority has the power to ensure ‘enhanced monitoring of the public spaces’[3] for accountability and crime reduction. The collected data is meant to be governed by the ‘Data and Privacy Protection Procedures (DP3)’[4], however the lack of transparency regarding the implementation of these procedures, and the recording and processing of citizens’ data is a source of concern for civil liberties.
2. In 2019 it was reported[5] that the Pakistani government had committed to procuring the services of Canadian company *Sandvine* for monitoring of Internet traffic in Pakistan using Deep Packet Inspection (DPI) on behalf of the Pakistan Telecommunication Authority (PTA) under the mandate of *Monitoring and Reconciliation of Telephony Traffic Regulations, 2010*. Though it was confirmed the Pakistani government had contracted[6] with *Sandvine,* the whole transaction is shrouded in lack of transparency.
3. FinFisher, an intrusion malware suite, was found to be operational in Pakistan, per computer forensic research conducted by The Citizen Lab[7].
4. CitizenLab in 2019 published a report[8] in which they used found NSO’s Pegasus spyware to be operational in 45 countries, where Pakistan was a part of the list as well. No further verifiable information could be found on this.

Communications surveillance is regulated by a number of laws in Pakistan:

- The *Investigation for Fair Trial Act (2013)* essentially legalises the use of technology to intercept and track devices by any authorised officer (BPS-20 and above) on issuance of warrant for surveillance by a judge of the High Court in order to successfully offences and be an indispensable aid to law enforcement as per the preamble of the Act
- The *Prevention of Electronic Crimes Act (2016)* includes sections enabling the extended retention of traffic data, the criminalization of defamation, and overall control over online content by the PTA
- The *Monitoring and Reconciliation of Telephony Traffic Regulations (2010)* through s.4 requires each long distance and international service provider to establish a system that allows for real-time monitoring and recording of traffic on PTA’s networks

[3] https://psca.gop.pk/about-us/benefits-and-objectives/

[4] https://psca.gop.pk/wp-content/uploads/2021/03/PrivacyPolicyDP3.pdf.

[5] https://www.codastory.com/authoritarian-tech/surveillance/pakistan-nationwide-web-monitoring/

[6] https://www.dawn.com/news/1484245

[7] https://citizenlab.ca/2015/03/finfisher-lawsuit-to-be-heard-in-pakistans-lahore-high-court/

[8] https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

- The *Pakistan Telecommunications (Re-organization) Act, 1996* allows for interception of calls and messages in the interest of national security (section 54(1))

A Guide about Surveillance of your Devices:

How Mobile Phone Extraction can be Used at a Protest and How to Minimise Risk to Data*

What do mobile phone extraction tools do?

- Mobile phone extraction (MPE) tools are devices that allow the police to extract data from mobile phones, including:
    - contacts;
    - call data (i.e. who you call, when, and for how long);
    - text messages (including who you texted and when);
    - stored files (photos, videos, audio files, documents etc);
    - app data (including the data stored on these apps);
    - location information history;
    - wifi network connections (which can reveal the locations of any place where you've connected to wifi, such as your workplace or a café).
- Some MPE tools may also access data stored in the Cloud (so even if you're very careful about minimising data stored on your device, it can still be accessed if it is stored online), or data you don't even know exists, and even deleted data.

How might mobile phone extraction tools be used at a protest?

- In order to extract the data stored on it, the police would need to physically access your mobile phone. The police might take your phone if you have been detained, arrested or searched during a protest, but also if you have witnessed or are even the victim of a crime

What to think about when going to a protest

- Keeping your phone's operating system (Android or iOS) up to date, which means it will have the latest security features, is likely the best way to prevent MPE.
- While the most effective way of protecting yourself against MPE is to not take your phone to a protest, this is unlikely to be a realistic solution. Indeed, not having your phone may leave you vulnerable in other ways. If you have an alternate phone with minimum data, it would be preferable to take.
- While you should keep your phone locked, some MPE tools are reportedly designed to access even locked phones. Their ability to bypass this security does, however, depend on the phone and its operating system.
- Before going to a protest, you may want to consider backing up your phone data to your computer, and then removing that data from your phone. But you should

be aware that some MPE tools are able to recover deleted data. If you have saved the data onto a cloud service, some MPE tools can still access that data.

How Cloud Extraction Tools Can be Used at a Protest and How You Can Minimise Risk to your Data

What are ‘cloud extraction tools’ and what do they do?

- Cloud extraction technology enables the police to access data stored in your ‘Cloud’ via your mobile phone or other devices.
- The use of cloud extraction tools means the police can access data that you store online. Examples of apps that store data in the Cloud include Slack, Instagram, Telegram, Twitter, Facebook and Uber.

How might cloud extraction tools be used at a protest?

- In order to extract your cloud data, the police would need to physically access your mobile phone. The police might confiscate your phone if you have been detained or arrested during a protest, but also if you have witnessed a crime and even if you are a victim of a crime (See also Protest Guide about mobile phone extraction).
- All of this information could be used to identify protesters and organisers and find out about the location of protests and actions.
- Your cloud data does not just reveal information about you, it can also reveal much about your friends, family, and anyone else you interact with online, such as fellow protestors. For example, you may have old contacts stored in the Cloud, which have been deleted from the phone itself.

What to think about when going to a protest?

- While you could consider leaving your phone at home, if that is not a realistic solution, you should think about switching off cloud back-up in the applications on your phone that you use, and logging out of all cloud-based services. This will avoid data being stored in the Cloud and prevent access to this data from your mobile phone.
- Before going to a protest, you should be aware that even if you use end-to-end encrypted messaging through WhatsApp, if you back up your WhatsApp messages to the Cloud, these encrypted backups could be accessed by the police using cloud extraction tools on your phone.

- Some applications, such as Uber, Twitter, WhatsApp and Facebook will allow you to switch off location data being stored in the Cloud. This may prevent the police being able to track where you have been.

How IMSI Catchers can be Used at a Protest and How Can You Minimise Risks to Your Data

In 2015, the Punjab Information Technology Board (PITB) set out a tender notice[9] for procurement of IMSI catchers for deployment in Counter Terrorism Departments (CTDs) of Punjab Police.

What is an IMSI Catcher?

- 'IMSI' stands for 'international mobile subscriber identity', a number unique to your SIM card. IMSI catchers are also known as 'Stingrays'.
- An 'IMSI catcher' is a device that tricks all mobile phones in its vicinity to connect to it in order to track them, by 'catching' their unique IMSI number.
- It does this by pretending to be a mobile phone tower with superb signal strength, tricking mobile phones nearby to connect to it, enabling it to then intercept the data from that phone to the cell tower without the phone user's knowledge.
- The most accessible information about you in this situation is your location. It is unavoidable that cell towers know your rough location through triangulation - indeed, this is how they provide you with their service in the first place. By putting itself between you and the cell tower, an IMSI catcher can work out your rough location.
- IMSI catchers do not read data stored on a phone. Instead, these devices can be used to try to intercept text messages and phone calls.
- Depending on the IMSI catcher's capabilities and on the network your phone is connecting to, more advanced attacks could take place, even though this is unlikely. Some Stingray devices rely on known weaknesses of communication protocols and can force your phone to downgrade the protocols it is using, to make your communications less secure and more easily accessible (e.g. by downgrading communications over 3G to 2G).
- IMSI catchers cannot read the contents of encrypted messages you exchange through platforms that use end-to-end encryption (e.g. Signal, WhatsApp, Wire).

[9] https://eproc.punjab.gov.pk/BiddingDocuments/35144_Tender%20Doc%20-%20Security%20Items%20for%20CTD%20Police%20Stations%20-%20105052015-1.pdf

How might IMSI catchers be used at a protest?

- The police can use IMSI catchers to identify who was at a protest, by capturing the IMSI numbers of all the phones that were in its vicinity at that protest.
- Some types of IMSI catchers can even enable the police to disrupt or prevent protests before they even happen.
- For example, they can be used to monitor or block your calls and messages; edit your messages without your knowledge; or even write and send someone messages pretending to be from you.

What to think about when going to a protest

- Putting your phone into airplane mode or switching it off completely will mean that an IMSI catcher can't track you or your communications.
- If you want to prevent the content of your text messages being tracked by an IMSI catcher, you can use messaging services that use end-to-end encryption, such as Signal and WhatsApp. The only information an IMSI catcher could potentially collect is the fact that you are using these messaging apps, not the content itself.
- While IMSI catchers do not read data stored on the phone, do bear in mind that the police may have other technology that could enable them to access data on your phone, such as 'mobile phone extraction' and hacking tools.

How Social Media Monitoring Can be Used at a Protest and How You Can Minimise Risks to Your Data

What is social media monitoring?

- Social media monitoring refers to the monitoring, gathering and analysis of information shared on social media platforms, such as Facebook, Twitter, Instagram and Reddit.
- It may include snooping on content posted to public or private groups or pages. It may also involve "scraping" – grabbing all the data from a social media platform, including content you post and data about your behaviour (such as what you like and share).
- Through scraping and other tools, social media monitoring permits the collection and analysis of a large pool of social media data, which can be used to generate profiles and predictions about users.

How is social media monitoring used in relation to protests?

- Protest organisers will often use social media to organise protests, communicate with protestors, and upload photos and videos of protests.

- In turn this means the police can ‘data mine’ social media pages and groups to try and learn the identities and affiliations of the organisers, the location and timing of a planned action, and other related information.
- The police may track social media posts relating to past or future protests to identify protesters.
- The police might also apply facial recognition technology or gait recognition technology to protest images and videos uploaded to social media to identify protestors.

What to think about when going to a protest?

- If you upload your protest images to your social media accounts, they may be used to identify and place individuals at the scene of a protest.
- If your location settings are switched on for your social media platforms or your camera and photo apps, and you then post online from or near the site of a protest, police may gain access to that location data.
- If you want to use social media while at a protest, you should consider switching off your location settings on the platform(s) you will be using. If you do decide to share protest images, do not tag individuals that were involved in the protest without their consent, as this could create a trail that police may rely on to place people at the protest.
- If you want to upload your protest images to social media accounts, consider removing the EXIF data beforehand. EXIF data is metadata associated with your images that can reveal information such as the location, time and date and device used.
- Be wary, footage can still be geolocated from background information (e.g. a monument or landmark). Keep this in mind when filming your surroundings and try to avoid identifiable backgrounds.
- If possible, upload pictures and videos only after you have left the location to safeguard against being tracked or followed and use a VPN to when uploading any visual data you may have recorded.

How Hacking Can be Used at Protests and How You Can Minimise Risks to Your Data

What is hacking?

- Hacking refers to finding vulnerabilities in systems, either to report and repair them, or to exploit them.

- Hacking can help to identify security flaws in devices, networks and services that millions of people use, and when reported to the system designers usually ends up with a fix in place. But hacking can also be used to access our devices in order to surreptitiously collect information about us, and potentially manipulate us and our devices in other ways.
- Hacking comprises a range of ever-evolving techniques. It can be done remotely, but it can also include physical interference with a device or system – for instance by forcing a mobile phone to unlock.
- It can also involve taking advantage of people to gain access to their technology. An example would be 'phishing', where an attacker impersonates a trusted person or organisation to send a link or attachment infected with malware.
- Hacking malware such as Pegasus has been reported[10] to have been used in Pakistan and 44 other countries, in a 2019 report by Citizen Lab. Pegasus technology can potentially be used to infect a mass number of iOS and Android devices.

How can hacking be used at protests?

- The police are able to hack into communications through the use of, for example, 'IMSI catchers'. But IMSI catchers can only intercept information that is being transmitted between a mobile device and a cell tower; IMSI catchers can't access information that is stored on the device.
- So the police can use sophisticated hacking techniques to get remote access to information stored on a phone, laptop or other Internet connected device used to organise or participate in protests, even if they are secured with a password, fingerprint or face unlock.
- The police may also collect and gain access to any devices that are dropped, lost or confiscated from protesters at a protest.

What to think about when going to a protest

- Keeping your device up to date is a good way to prevent hacking, as hacking often exploits vulnerabilities that have been disclosed but not yet patched.
- Ensure that your device is running the latest available version of its operating system (Android or iOS) and that all your apps are up to date to improve your security and minimise the risk of hacking.
- While you should keep your phone or other electronic devices locked, some hacking techniques can access even locked devices. Their ability to bypass this

[10] https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

security, this however, depends on the hacking technique used and the device it targets.

- Before going to a protest, you may want to consider backing up your phone data to another device, and then removing that data from the devices you take with you. But you should be aware that some hacking tools are able to recover deleted data. If you have saved the data onto a cloud service, some hacking tools can still access that data.
- You should always be careful about what links you click, to avoid ‘phishing’ attacks.

A Guide to Surveillance of your Face and Body

How Facial Recognition can be Used at a Protest and How You can Try to Maintain your Anonymity

What is Facial Recognition Technology?

- Facial recognition technology (FRT) collects and processes data about people's faces, and can be used to identify people. FRT matches captured images with images stored in existing databases or 'watchlists'. Pakistan Customs Department was reported[11] to be putting in place a National Targeting Centre (NTC) relying on facial recognition technology which would be linked with multiple government entities including the Immigration Department, NADRA, Advance Passenger Information System, National Customs Enforcement Network among others, to assist Pakistan Customs and assist law enforcement agencies in profiling potentially risky individuals and conveyances.

How might it be used in relation to a protest?

- FRT may be used to monitor, track and identify people's faces in public spaces, including at protests. This may be done openly or surreptitiously, without people knowing or consenting.
- FRT-enabled cameras can take pictures or videos, and identify people in real-time or at a later point. FRT can also be used to analyse and identify existing images, for example photos and videos of protests uploaded to social media.
- As protesters' face data is collected, this data can then be added to one or more preexisting watchlists, where it can be compared against face data from other sources to find a match.
- Such data could also potentially be used to create a new database of people who attend protests for future matching and identification.

What to think about when going to a protest?

- If you want to try to maintain your anonymity, you may want to consider wearing a face covering such as a mask, which may make it harder for FRT to capture accurate images of your facial features.
- Other options for disrupting FRT include the use of face paint and clothes with designs meant to interfere with accurate facial recognition. FRT is constantly changing and improving, however, so face coverings and these other methods may prove less effective in the future.

[11] https://www.dawn.com/news/1584264

- Police powers to demand the removal of such coverings and clothing vary depending on the cultural context and jurisdiction. At the time of writing, we are in the midst of the Coronavirus epidemic, so current rules may be subject to change.
- As the police can use FRT to analyse images or video recordings on social media, consider this carefully before you post any images from a protest that feature the faces of other protestors.
- As such, you may want to consider using face blurring tools before posting photos or videos online.

How Police Drones Technology can be Used at a Protest and how you can try to maintain your anonymity

Islamabad Capital Police announced procurement of such ‘non-lethal’ drones to ‘to limit and regulate public gatherings to maintain law and order’[12] in September of 2022.

What are police drones?

- Drones are remotely controlled Unmanned Aerial Vehicles (UAVs) of varying sizes.
- They usually come equipped with cameras and might be enabled with Facial Recognition Technology.
- Drones can be equipped with speakers, surveillance equipment, radar and communications interception tools, such as ‘IMSI catchers’.

How might drones be used during protests?

- Camera-enabled drones may be used to remotely monitor and track people’s movements in public spaces, including at protests, without them consenting or even knowing.
- Similarly, when equipped with communication interception technologies, drones can be used to monitor and track protestors’ calls and messages, in and around the area where a protest is taking place.
- Drones equipped with speakers may also be used to communicate with protesters, for example by giving them orders, instructions or warnings

[12] https://tribune.com.pk/story/2375942/islamabad-police-to-use-non-lethal-drones-to-disperse-rioters

What to think about when going to a protest?

- Drones' use and impact on your anonymity depends on the technologies they are equipped with.
- See sections above covering Facial Recognition Technology and IMSI catchers, as these are common tools that a drone could use to monitor the activities of protestors.

A Guide to Policing Databases and Predictive Policing Tools

What is Predictive Policing?

- Predictive policing programs are used by the police to estimate where and when crimes are likely to be committed – or who is likely to commit them. These programs work by feeding historic policing data through computer algorithms.
- For example, a program might evaluate data about past crimes to predict where future crimes will happen – identifying ‘hot spots’ or ‘boxes’ on a map. But the data these programs use can be incomplete or biased, leading to a ‘feedback loop’ – sending officers to communities that are already over-policed.
- Other predictive policing programs may suggest how people will behave. These programs are fed information about a person, and then they decide whether that person is likely to commit an offence.
- The Ministry of Information Technology and Telecommunications (MOITT) has recently launched the “Crime Analytics and Smart Policing in Pakistan (CASPP)” which aims to use data analytics to perform predictive policing functions.[13] The program will be rolled out across major cities across the country, namely Karachi, Islamabad, Gilgit, Muzaffarabad and Quetta.[14]

How can Predictive Policing be Used at a Protest?

- The police may use facial recognition technology, IMSI catchers or geo-location technology to identify protesters and add them to databases or watchlists.
- Individuals are also often unaware if they have been included on a Police database or a watchlist and as a result, their removal from it is very difficult, if not impossible. What to think about when going to a protest.
- Any photos, videos or messages that you share about a protest on any online platform may be analysed by the police to identify protesters. Once identified, they can then be added to watchlists or used to create profiles that then can feed into predictive policing tools.

[13] “Changes underway for a unified, integrated policing system in country: Amin-ul-Haque”, The Nation, August 20, 2022, https://www.nation.com.pk/20-Aug-2022/changes-underway-for-a-unified-integrated-policing-system-in-country-amin-ul-haque.

[14] Muhammad Saleh Zaafir, “Crime analytics and smart policing to be implemented in Pakistan: Aminul Haq,” The News International, August 24, 2022, https://www.thenews.com.pk/print/984957-crime-analytics-and-smart-policing-to-be-implemented-in-pakistan-aminul-haq.

- If police have already classified you as someone that is likely to commit a crime, this may further be used to detain, arrest, or stop and search you during a protest.
- The lack of transparency from the government in general and the dearth of open government policies adds to the potential of misuse of these databases.

How Law Enforcement Databases can be Used at a Protest

The Punjab Police Integrated Control and Command Centre (PPIC3) under the Punjab Safe Cities Authority (PSCA) is an entity with a mandate to collect data for purposes of enhancing the level of security provided to citizens. This includes the installation of CCTV, predictive policing measures by identifying areas with greater instances of criminal incidents.

This system was initially deployed in Lahore and by now is present in 6 other cities (Islamabad, Bahawalpur, Multan, Faisalabad, Gujranwala, Rawalpindi) at least, with plans for expansion.

Given the scope under which PSCA operates, with reports of 10,000 cameras being installed in Karachi too, and the purported element of 'security' as their guiding principle, it is possible that the database of footage produced over the years can be used to surveil protests taking place in these cities.

In addition to predictive policing programs launched by the MOITT, it has also launched multiple initiatives for digitization in attempts to curtail crime, such as Hotel Eye and Travel Eye as well as widespread digitization of police stations,[15] FIR (First Instance Report) registration and complaint mechanisms, amongst others.[16] The source of concern here is the widespread collection of personal data in a country where no laws

[15] Muhammad Saleh Zaafir, "Crime analytics and smart policing to be implemented in Pakistan: Aminul Haq," The News International, August 24, 2022, https://www.thenews.com.pk/print/984957-crime-analytics-and-smart-policing-to-be-implemented-in-pakistan-aminul-haq.

[16] Muhammad Shahzad, "Police stations across Punjab going digital," March 12, 2017, https://tribune.com.pk/story/1353012/police-stations-across-punjab-going-digital.
Manzoor Ali, "Police dept digitises over 1.43m FIRs," Dawn, October 7, 2018, https://www.dawn.com/news/1437332.
"KP CM inaugurates e-FIR, digitisation of police HR management system," The News International, February 7, 2020, https://www.thenews.com.pk/print/610235-kp-cm-inaugurates-e-fir-digitisation-of-police-hr-management-system.

govern this collection and the subsequent processing and maintenance of these databases.

A Guide to Protect your Devices against Surveillance

How to Better Control Access to Data Location

Where is my phone location stored?

Your phone can find its location in two main ways, using GPS or mobile network location:

1. GPS:
    a. GPS (Global Positioning System) uses satellite navigation to locate your phone fairly precisely (within a few metres), and relies on a GPS chip inside your handset.
    b. Depending on the phone you use, your GPS location data might be stored locally and/or on a cloud service like Google Cloud or iCloud. It might also be collected by any app that you use that has access to your GPS location.
2. Mobile network location:
    a. Mobile network location (or Global System for Mobile Communications (GSM) localisation) relies on your cellular network, and can be determined as soon as you are connected to the network (i.e. your phone is switched on and not in airplane mode) but is far less precise than GPS. Your approximate location can be determined with an accuracy range of a few dozen metres in a city, or hundreds of metres in rural areas.
    b. This location data is stored by your network provider.

How can my location data be accessed?

There are a number of methods that can be used to can gain access to your (phone) location:

1. GPS:
    a. Accessing GPS location data depends on where the data is stored. It can be done using a ‘mobile phone extraction’ device, which plugs into your phone and downloads all the data stored on it, including details of locations you have visited.
    b. Access to your GPS data may also be possible through device hacking, an advanced technique which might not necessarily require physical access to your phone and could be done remotely.

    c. If your GPS data is also stored on an online account (e.g. iCloud or Google Maps), it can be accessed through cloud extraction technologies or legal requests to the companies that store that data.

2. Mobile network location:
    a. Your approximate location data can be accessed by the police through your service provider.
    b. This means that the police don’t need access to your phone handset to determine that you were within a certain proximity of a protest.
    c. Another means of accessing this same information is to use an ‘IMSI catcher’ (also known as a ‘Stingray’), a device deployed to intercept and track all mobile phones switched on and connected to a mobile network in a specific area.

How to better control your location data?

1. GPS:
    a. The best way to prevent your location being accessed is to limit the generation of the location data in the first place.
    b. In the case of GPS, it can be as simple as switching off your GPS (often referred to as ‘location services’). But bear in mind that the location data of any previous occasions where you did have it switched on might still be accessible.
    c. You may still need to use GPS on your phone, for example if you’d want a friend or family member to be aware of your location as you attend a protest for safety purposes. In that case, check individual apps’ permissions to access your location to minimise the spread of this information.
    d. Removing permissions to access your location for all apps can prevent this data being stored on an online account.
    e. If you absolutely need an app to have access to your GPS data, inspect the settings of that app to ensure that you understand if your location is being stored online or just locally on your app. For example, if you use Google Maps while logged into a Google account, you might want to disable location history in the settings so that your location history won’t be stored in your Google account.
    f. If you’ve taken pictures with your location services switched on, the location where the picture was taken might be included in the metadata (known as EXIF data) of the image. You might want to disable location services while taking pictures, or you can use software or an app to erase

this EXIF data afterwards (for example, the Signal messaging app erases EXIF data when you send images).

g. Similarly, turning off your wifi or Bluetooth can prevent your phone from connecting to unwanted access points and providing indirect location information.

2. Mobile network location:
    a. When it comes to mobile network location, the only way to have control over it is to prevent connection to the network at all.
    b. Having your phone switched off, in airplane mode, or in a faraday cage will prevent connection to your mobile network, and therefore make GSM geolocation impossible. A faraday cage or switching off your phone prevents any and all types of connection to any phone network. Whereas just using airplane mode means that some types of connections can still be made (e.g. Bluetooth or GPS).

How can the police gain access to your images, contacts and documents and how can you better control access?

Where is it all stored?

- You generate data every time you use your phone e.g. you generate data when you take photographs or record videos, when you create or edit notes and documents on the go, and when you add new names and numbers to your contacts directory.
- All this data is created through dedicated apps - your camera and photo apps, social media apps, notes apps, and your contacts app are just some examples.
- It is important to note that when you create any file on your phone, most of the time you will also generate ‘metadata’ that is coupled to it (e.g. a photo will have metadata such as the time and location it was shot). This metadata can be as revealing, if not more revealing, than the photo itself.
- All this data will be stored on your phone’s internal memory (including any external memory attached, such as a MicroSD card), or on the Cloud, or both if you are using any cloud services as a backup

How can my images, contacts and documents be accessed by the police?

There are a few ways the police can gain access to this data, depending on how it is stored:

- If you store all your data locally on your phone, then it can be accessed using a ‘mobile phone extraction’ device, which connects to your phone and downloads all the data stored in it. This method cannot be used remotely - the police would need physical access to your phone.

- Device hacking is an advanced technique that gives access to a certain amount of data in your phone, but not necessarily all of it. Unlike mobile phone extraction, hacking doesn't necessarily require physical access to your device. This means that this method can be used any time before or after a protest.
- If you are syncing your images, documents and contacts using any cloud services (iCloud, Dropbox or Google Drive for example), the police can use 'cloud extraction' tools remotely to access this information without your authorisation or knowledge, or they can make a legal request to the cloud service provider.

How to limit the risk of your images, contact and documents being accessed

- To prevent being targeted by cloud extraction techniques, you would need to refrain from using Cloud services altogether.
- If giving up Cloud services entirely is going to create too much inconvenience for you, consider not uploading sensitive content to the Cloud. Reviewing apps' settings and features is also a good way to ensure you know what data on your phone is being backed-up online (for example, WhatsApp backups can be stored on Google Drive, so even though your WhatsApp messages are end-to-end encrypted, using cloud extraction tools these messages could still be accessed from your Google Drive backup).
- However, as the device user, you have some control over the data you generate in the first place, and where it is stored. Having a good understanding of what information your phone holds about you means that if such tools were to be used on your phone, you are more likely to be aware of what data is being accessed.
- Ensuring the content of your phone is encrypted and that your operating system and apps are up to date will mitigate against some methods of mobile phone extraction and device hacking.

Digital Communications:

Where are my communications stored?

- Text messages/phone calls: Traditional cellphone communications happen over the cellular network. You usually access those with the text message and phone call apps that are provided as standard on your phone. While phone calls aren't stored anywhere, text messages are stored locally on your and the recipient's devices. They might also be temporarily stored by the network provider.

- Messaging apps: Messaging platforms enable fairly secure communication over the Internet. Depending on the app you use, your messages might be stored locally on your and the recipient's phone, on the service provider's systems, and potentially online too. Some messaging apps also offer backup solutions which will be stored either online or locally. Different messaging apps also rely on different protocols, which means that some messaging apps are more at risk of interception than others.
- Social networks: Except in rare cases of decentralised/self-hosted systems, your communications on social networking apps will be stored by the service providers.

How can my communications be accessed?

There are a few ways the police can gain access to this data, depending on where you have it stored:

- Accessing the communications stored on your phone (such as your conversations in a text messaging app) can be done through a 'mobile phone extraction' device, which can be connected to your phone to download all the data stored on it.
- Such access may also be possible with device hacking, a technique which may not require physical access to your phone.
- If your communications rely on a service provider or a social network (such as Messenger, Telegram, Instagram, TikTok), the police can gain access through 'cloud extraction' technologies, without your consent or knowledge. The same technique can be used to access backups of your communication (e.g. WhatsApp backups on Google Drive/iCloud).
- If some of your communications on social networks are public (e.g. shared on an open Facebook group), the police can also use Social Media Intelligence (SOCMINT) tools to access them.
- Your text messages and phone calls can be intercepted, recorded and interfered with by the police using an 'IMSI catcher', a device deployed to track all mobile phones switched on and connected to the network in a specific area.
- Your text messages can also be accessed through a legal process targeting your service provider. Similar legal processes can be used to request data from companies that might host your communications (e.g. Facebook).

How to limit risk of communications being accessed?

- Limiting the risks starts with controlling the amount and type of information you share, with whom and through which medium.

- When sharing very sensitive information, consider meeting in person.
- If meeting in person is not an option, given the low security of cellular networks, consider the use of secure channels such as end-to-end encrypted messaging apps to share sensitive information.
- But do bear in mind that if you use cloud backup for any of your messaging apps, the content could still be accessed using cloud extraction tools.
- Verify the identity of protestors you are communicating with through a different communications channel (e.g. messaging them on another platform, or over encrypted email, or over a voice or video call).

Unique Identifiers: What are they and where are they stored?

- Your phone and your SIM card contain unique identifiers about you, which can be accessed by the police to identify you.
- The IMSI (International Mobile Subscriber Identity) is a unique number associated with your SIM card. It doesn't change, even if you put the SIM card into a different phone.
- If you have a mobile phone subscription, the IMSI will be associated with personal information such as your name and address.
- The IMEI (International Mobile Equipment Identity) is a unique number identifying your phone (the device). So if you change your phone, you will have a new IMEI.
- IMSI and IMEI cannot be easily altered without a specialist tool, and they can be linked to information about you (e.g. name, address) or your device (e.g. brand, model).
- Ad ID: Ad Identifiers are different from IMSI and IMEI in that they can change over time. Ad IDs are used by advertisers in apps and websites to uniquely identify you online and offer services such as targeted advertising. Ad IDs are not directly linked to your personal information (e.g. your name) but can be associated with other revealing data about you (e.g. geolocation, apps used, websites visited etc). The Ad ID is generated by your phone's operating system, and is usually visible in the settings of your phone. It can be manually renewed.
- Other identifiers: There are a few other components in your phone with supposedly globally unique identifiers, such as the MAC address for your Wi-Fi, or the BD_ADDR for your Bluetooth module.

How can the unique identifiers be accessed?

- Your IMSI and IMEI can be obtained by the police with an 'IMSI catcher', a device deployed to track all mobile phones switched on and connected to the network in its vicinity. Once this identifier is intercepted, it might be used to retrieve personal information about you.

- Your Ad ID can be accessed by apps and websites on your phone. While it is not directly associated with your personal information (e.g. your name and address), it can be associated with other data such as your location. Some data brokers obtain massive amounts of data from phones and sell it to the police, including the Ad ID.
- Other unique identifiers such as your MAC address can be collected by wifi hotspots but it is far more difficult to associate this with personal information that can be used to identify you, and recent iOS and Android releases will spoof your MAC address when connecting to a new, unknown network.

How to limit risk of being identified by ‘unique identifiers’?

- If you are in a situation such as a protest, where you may want to ward off the risk of an IMSI catcher tracking your phone, the most effective option would be to refrain from connecting to the cellular network. Having your phone in airplane mode or in a faraday cage will make you invisible to cellular towers, and therefore to IMSI catchers as well.
- If it’s important that you are connected to the cellular network, consider getting a separate prepaid SIM card, (because you provide very little information when you buy a prepaid SIM card). If you do so, note that if your phone connects to a police IMSI catcher at different times with these different SIM cards, it will be possible to tie the pre-paid SIM to the identity registered under your original SIM card. This is because of the IMEI, the unique identifier of your phone.
- Renewing your Ad ID on a regular basis is a good way to avoid all your phone activities being gathered under the same ID. You might also want to disable personalised advertising if your mobile offers this option as it will prevent apps and websites from obtaining this identifier.
- Using an Ad Blocker is also a good way to prevent companies from tracking you online and collecting your personal information.

Fact Sheet on your Data Rights in Relation to Police Surveillance at Protests

- Prevention of Electronic Crimes Act (2016)

Section 35 (2) directs officers dealing with devices and data to a) act with proportionality b) take measures to protect secrecy of any information system they have access to in exercising their power to search and seize.

Section 36 directs officers on how to deal with seized information systems including listing down what items have been seized and providing the list to the owner or possessor of the information systems and data.

Section 41 speaks to confidentiality of information and lays out a three year imprisonment term and/or fine up to one million rupees for any person, service provider or authorised investigation officer who discloses data without consent or in breach of contractual obligations with intent to cause or knowing he may cause harm, loss, gain to any person or compromise confidentiality of such material or data.

- Right to Information (RTI) Laws

Pakistan now has RTI laws for all four provinces and at the federal level to allow access to information and records held by public bodies, pursuant to Article 19A of the Constitution of Pakistan 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.’

Federal: Right of Access to Information Act 2017

Punjab: The Punjab Transparency and Right to Information Act 2013

Khyber Pakhtunkhwa: KP Right to Information Act 2013

Sindh: Sindh Transparency and Right To Information Act 2016

Balochistan: Balochistan Right to Information Act 2021

Individuals and organisations can approach Information Commissioners with regards to each jurisdiction to make requests for information. The overriding caveats and exceptions in these legal instruments include but are not limited to restricting disclosure of information if it can lead to commission of an offence, hamper case inquiries or affect national security considerations.

Photographing Police Officers at a Protest

While a policy directive was issued by the Inspector General of the Punjab Police banning mobile phones, laptops and cameras at all police stations in Punjab in 2017[17], no clear policy or rule exists as per our existing knowledge that criminalises the photography of police officers at a protest. Since protests are public gatherings, restrictions on photography could run afoul of freedom of expression safeguards. Instances of using photographic and videographic evidence of unconstitutional, excessive behaviour exercised by police officers to call attention to use of disproportionate force have been recorded[18] to employ as a tool for demanding accountability.

Regardless of the fact that taking photographs of, filming or otherwise recording the conduct of police officers is not outlawed, caution must be exercised by protesters when carrying out these activities to avoid risks to safety.

*Note: There is no publicly available information that Pakistan law enforcement is deploying MPE tools, however we cannot exclude its occurrence based on the existence of generic search and seize powers.

[17] https://www.dawn.com/news/1353555

[18] https://www.dawn.com/news/1694624