A GUIDE TO AVOIDING UNLAWFUL TECHNOLOGICAL INTERFERENCE IN THE EXERCISE OF FREEDOM OF EXPRESSION

TURKISH EDITION



privacyinternational.org

With today's technology, it is seen that the ways of using freedom of expression have also developed, and although it is thought that freedom of expression has become stronger, it has become more open to external interventions. In addition to the legal-criminal dimension of these interventions, there is also the possibility of personal data being captured by malicious people. It is also observed that such dangers prevent the effective exercise of freedom of expression and that individuals practice self-censorship in order to avoid such dangers.

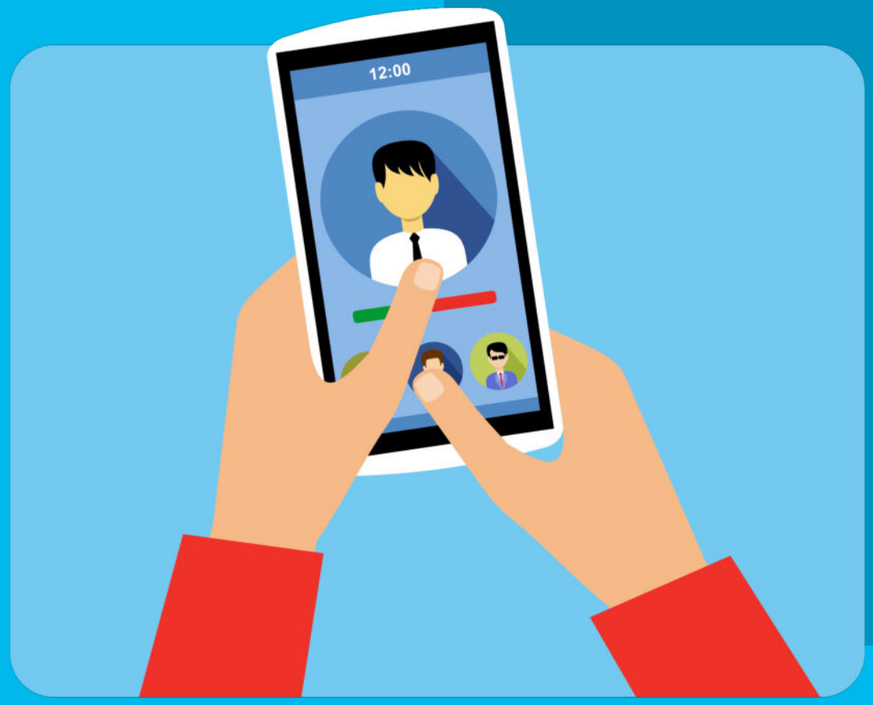
We must be free to exercise our freedom of expression.

This guide is also an attempt to provide basic tools for people to protect themselves when exercising various forms of freedom of expression - but even then, it only outlines what is really needed to ensure that people can safely carry out their vital work.

This guide has been created in cooperation with local activists and Privacy International, adapting the UK Freedom of Protest Guidelines to Turkish laws and policies. It is not intended as a substitute for legal advice and serves only to set out a range of information on and around the security of freedom of expression. We hope that it will be a drop in the sea of advocacy for the free and effective exercise of freedom of expression.

Social Media Monitoring





74z6j20n
f36rq928

KEY FINDINGS

- Social media is important for the exercise of freedom of expression and people rely on social media to express themselves.
- With the developing technology, people are exposed to technology-based surveillance, and online activities are observed as a key carrier of surveillance,
- This guide aims to provide mitigating measures that can enable individuals to continue to use the tools necessary for their work.

We wanted to provide some information that citizens can use to avoid social media monitoring so that you can be freer to express yourself.

Restricting the amount of personal information you share online

• Social media plays a key role in bringing like-minded people together, organising them and bringing about change.

• While social media activities are undoubtedly useful for self-expression and participation in social issues, they are not without risks - activities on social media platforms can leave a footprint that other actors may want to follow or exploit. It is therefore useful to limit the sharing of personal information.

Social media monitoring

Social media monitoring refers to monitoring, collecting and analysing information shared on social media platforms such as Facebook, Twitter, Instagram and Reddit. Such monitoring may include scanning content posted in public or private groups or pages. It may also include "scraping", which involves retrieving all data from a social media platform, including content you post and data about your behaviour (such as what you like and share). Social media monitoring through scraping and other means allows for the collection and analysis of a large pool of social media data that can be used to build profiles and predictions about users.

The way you interact with social media sites can reveal a lot about you, sometimes without you realising it, and unless you change your privacy settings in a specific way, your data becomes more vulnerable to social media monitoring. There are general good practices and settings on your social media accounts that can protect your privacy and make it harder for third parties to spy on your activities.
The following good practice measures apply to all social media sites, whether Twitter, Facebook or Instagram.

Security

- Consider enabling two-factor authentication (also known as 2FA). This provides an extra step of security to access your account. This way, when you connect, your social media account will verify your identity by asking for a code in addition to your username and password.
- Enabling password reset protection will prevent anyone trying to hack your account from accessing your personal data, such as your mobile phone number/email address to which the reset code will be sent.
- If you log in to your account from other devices (public/shared), be sure to log out each time.
- If the app you use allows file sharing, be careful before downloading anything sent to you (such as a file or document that needs to be opened on your phone) or clicking on links sent by people you don't know or trust.

Privacy settings

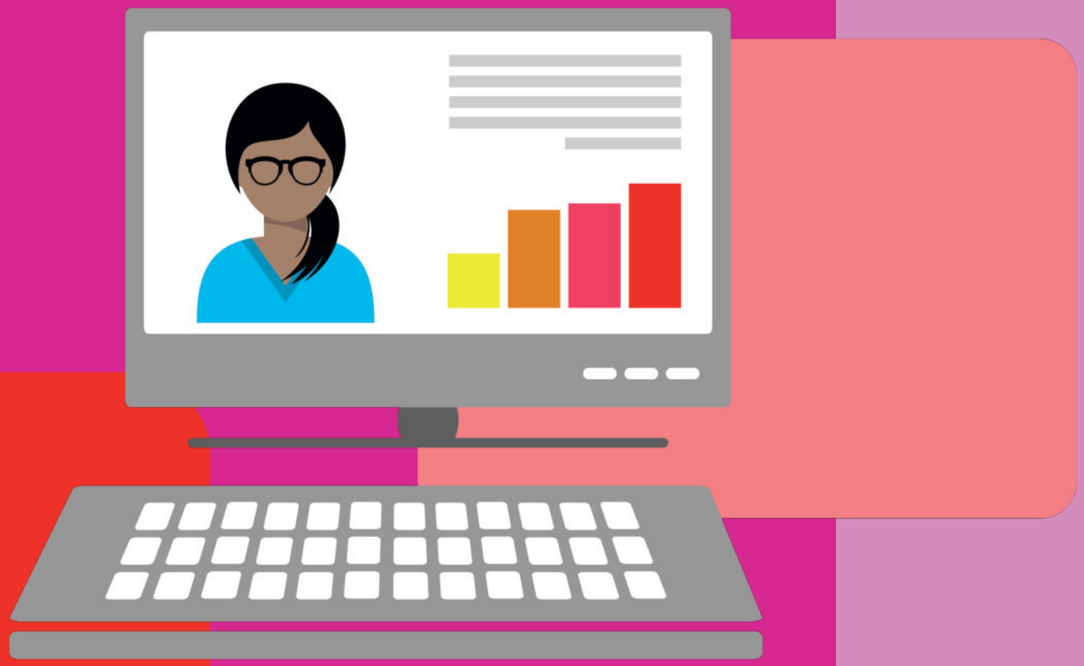
- It is a good idea to review the privacy settings of the social media platforms or apps you use whenever possible. In particular, consider reviewing whether the platforms or apps you use share data with third parties and use your discretion when authorising the sharing of such data.
- Consider enabling settings that restrict allowing people to tag you in photos without your permission.
- Consider enabling privacy mode where possible and do not accept follow requests from unknown accounts.

What you should pay attention to when sharing

- Be careful with sensitive information you share in your photos or captions.
- Be aware of the location settings on your devices and consider that your location may be revealed by background details. Similarly, consider reviewing any data that may have been uploaded with your images and delete or modify it as necessary.
- If you want to use hashtags, consider what private data about you (or location) they might reveal.
- If you want to remain anonymous, consider not sharing personal data that could damage your anonymity, such as your date of birth, place of birth, age, where you live, occupation, education, etc.
- Be careful when sharing photos of children on social media.

Messaging - Apps and Social Media





GUIDE TO COMMUNICATING WITH OTHERS: MESSAGING APPS

Messaging apps have become an important part of the way we communicate with each other in all aspects of our lives, from communicating with distant relatives, to socialising, to getting involved in politics. Some of these applications include Facebook Messenger, Twitter DM, Whatsapp, Signal, Telegram and Viber. These apps can be used for private chats as well as to create group chats for the exercise of constitutional rights, ranging from solo actions to organising mass gatherings and peaceful protests. It is therefore important that people use apps for their safety that are commensurate with their trust in these apps. However, there are so many apps that it is difficult to know which ones are the safest.

Check out our guide below to learn more:
What are the key factors to consider when using a messaging app?
There are two main things to consider when deciding which messaging app you want to use:

1. Whether it offers end-to-end encryption that protects the content of your communications; and
2. Whether it collects any information beyond the message content, such as location, who you are communicating with and other details called 'metadata'.

Why is encrypted messaging important?

Encryption is the process of scrambling information so that it cannot be read by anyone other than the sender and the intended recipient(s). The use of cryptography to communicate secretly dates back to ancient Egypt and continues to the present day.

End-to-End Encryption ("E2EE") describes the process of sending encrypted content from one receiver ("end") to another in such a way that the content cannot be read or altered by third parties in transit. E2EE continuously protects the confidentiality and integrity of the transmitted information by encrypting it at the source and decrypting it at the destination. When E2EE is used, service providers cannot intercept the content or read the messages because they remain encrypted even when travelling through service providers' servers. In fact, anyone trying to intercept the message in transit before it reaches the recipient's device cannot read or modify its content.

E2EE is made more assured by the use of digital signatures, where messages are signed to prove who wrote them.

It is important to note that with almost all messaging apps, when messages are received, your phone will decrypt them, save them and show them to you in the app as decrypted. As a result, encrypted messaging does not protect you from someone accessing your phone to read your messages.

Therefore, for sensitive conversations, it may make sense to use disappearing / scheduled / vanishing messages if offered by your application as a method to stop long-term storage of messages. However, it is also important to remember that any recipient in a conversation can take a screenshot or store the message in some other way. In addition, the application displays a notification that message deletion has occurred and shows placeholders for manually deleted messages. It is unclear whether self-destructing messages can also be recovered by mobile phone extraction technology.

Note, however, that apps like Twitter collect data about Direct Messages, including how you interact with others on the platform, such as people you follow and people who follow you, metadata about encrypted messages and the content of messages, recipients, and the date and time of messages.[1]

You may want to consider E2EE for messaging in light of the higher security they provide compared to text messages/SMSs. SMS messages are completely unencrypted, meaning they can be easily read, manipulated or forged in transit. They can also be stored by your telecommunications provider, which may be subject to access requests from people who want to spy on you.

[1] https://x.com/en/privacy

Does your app encrypt both content and contact data?

Another aspect to consider when choosing an application is metadata generation - data about what, to whom and when you send your messages, rather than the content of your messages.

Signal uses E2EE not only to encrypt the content of messages, but also to hide all metadata even from itself, storing only when an account was created and when it last connected to the service.

In contrast, both WhatsApp and Telegram store and can access much more metadata, including IP addresses, profile photos, "social graphs" and more.

In Telegram's case, Telegram does not use E2EE by default, instead storing all messages with keys over which they have full control. As a result, Telegram can access messages at any time. The cases in which both WhatsApp and Telegram have occasionally responded to police requests for information show that the provider companies have access to these messages.

WhatsApp also collects information about how you interact with others, as well as the features you use, such as groups or search, but like Signal, they do not keep encrypted messages on their servers after they are delivered, and they delete undelivered messages after 30 days.

Your app may require your phone number to use it

To reduce the number of steps in the registration queue, most messaging apps rely on a phone number. While this is useful for more widespread use, it may not be ideal for people who do not want to provide their personal number.
There are ways to avoid this, such as signing up for a messaging app using the number of an alternative SIM card you have.

Chat backup

Some applications may offer chat backup as an option. While backup is desirable for many people to prevent their messages from being lost, backup on the Cloud can pose a potential threat to users' privacy, as anyone with access to your Apple (if backed up on iCloud) or Google account (if backed up on Android) can access it.

If you choose not to keep backups, this should mean that your messages only exist within the app, which minimises the attack surface.

Minimise your profile information

Messaging apps often allow you to keep a profile, which may include a photo, a status or an 'about' section.

If you intend to communicate with people you don't trust, this information may reveal things about you that you want to keep private. As a general rule, you may want to consider choosing the most private option offered.

In most cases, limiting the visibility of these details to your 'contacts' may be a good option, but if you intend to use the messaging app to connect with people you don't know, it may be worth keeping any profile settings to a minimum or blank.

Application	E2EE Offers	E2EE by Default	Requires a telephone number
iMessage	Yes	When not stored in the cloud	Yes
WhatsApp	Yes	Yes	Yes
Signal	Yes	Yes	Yes
Viber	Yes	Yes	Yes
Telegram	A little bit	No	Yes
Skype	Yes	No	No
Wickr	Yes	Yes	No
Matrix Customer	Customer Based	When offered by the customer	No
Facebook Messenger	Yes	No	Increasingly
Google Messages	Yes	Yes	No
Instagram DMs	Yes	No	No
Twitter DMs	No	No	Increasingly
Discord	No	No	No

AVOIDING SURVEILLANCE



MOBILE PHONE EXTRACTION AND HOW TO MINIMISE THE RISKS TO YOUR DATA

What are mobile phone removal tools for?

• Mobile phone extraction (MPE) tools are devices that enable data extraction from mobile phones, including:
- Persons;
- search data (i.e. who you searched for, when and for how long)
- text messages (including to whom and when you sent a message);
- stored files (photos, videos, audio files, documents, etc.)
-application data (including data stored in these applications);
- location information history;
- wifi network connections (can reveal the location of any place where you connect to wifi, such as your workplace or a cafe).

• Some MPE tools can also access data stored in the Cloud (so even if you are very careful about minimising the data stored on your device, it can still be accessed if it is stored online) or data that you did not even know existed, or even deleted data.



What should you pay attention to?

• Keeping your phone's operating system (Android or iOS) up to date, i.e. having the latest security features, is probably the best way to prevent MPE.

• While the most effective way to protect yourself against MPE is to not take your phone to places where you might be unsafe, this is unlikely to be a realistic solution. In fact, not having your phone with you can leave you vulnerable in other ways.

• While you should keep your phone locked, some MPE tools are reportedly designed to access even locked phones. However, the ability of these tools to bypass this security depends on the phone and operating system.

• You may consider backing up your phone data to your computer and then removing this data from your phone. However, you should be aware that some MPE tools can recover deleted data. If you have saved the data to a cloud service, some MPE tools can still access it.

CLOUD EXTRACTION TOOLS AND HOW TO MINIMISE RISKS TO YOUR DATA

What are 'cloud extraction tools' and what do they do?

• Cloud extraction technology enables access to data stored in your 'Cloud' via your mobile phone or other devices.

• Using cloud extraction tools means that malicious people can access the data you store online. Examples of applications that store data in the cloud are Slack, Instagram, Telegram, Twitter, Facebook and Uber.

What should you pay attention to?

• If you are in an insecure environment, you should consider switching off cloud backup in the applications you use on your phone and logging out of all cloud-based services. This will prevent data from being stored in the Cloud and access to this data from your mobile phone.

• Even if you use end-to-end encrypted messaging via WhatsApp, if you back up your WhatsApp messages to the Cloud, these encrypted backups can be accessed using cloud extraction tools on your phone.

• Some apps such as Uber, Twitter, WhatsApp and Facebook allow you to switch off location data stored in the Cloud. This can prevent malicious people from being able to track where you are.

IMSI CATCHERS AND HOW TO MINIMISE THE RISKS TO YOUR DATA

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 locates and then tracks all mobile phones connected to a telephone network in its vicinity by 'catching' the unique IMSI number.

• It does this by acting as a mobile phone tower, tricking nearby mobile phones into connecting to it, and then intercepting data from that phone to the base station without the phone user's knowledge.

• The most accessible information about you is then your location. It is inevitable that base stations will know your rough location through triangulation - in fact this is how they serve you in the first place. An IMSI catcher can get between you and the base station and determine your rough location.

• IMSI interceptors do not read the data stored on the phone. Instead, these devices can be used to try to intercept text messages and phone calls.

• Depending on the capabilities of the IMSI catcher and the network your phone is connected to, more sophisticated attacks may occur, but this is unlikely. Some Stingray devices exploit known weaknesses of communication protocols and can make your communications less secure and more easily accessible by forcing your phone to downgrade the protocols it uses (for example, by downgrading communication over 3G to 2G, because as far as we know, content interception and real-time decryption can only be performed when the target is connected over a 2G network).

• IMSI catchers cannot read the content of encrypted messages you share via platforms that use end-to-end encryption (e.g. Signal, WhatsApp, Wire).



What should you pay attention to?

• Putting your phone in aeroplane mode or switching it off completely will mean that the IMSI catcher will not be able to track you or your communications.

• If you want to prevent the content of your text messages from 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 that an IMSI catcher can potentially collect is the fact that you are using these messaging apps, not the content itself.

• Note that although IMSI catchers do not read the data stored on the phone, malicious people may have other technologies, such as 'mobile phone extraction' and hacking tools, that allow them to access the data on your phone.

1.

HACKING, AND HOW TO MINIMISE THE RISKS TO YOUR DATA

What is hacking?

• Hacking means finding, reporting and repairing or exploiting vulnerabilities in electronic systems.

• Hacking can help identify and fix vulnerabilities in devices, networks and services that millions of people may use. But it can also be used to access our devices, collect information about us and manipulate us and our devices in other ways.

• Hacking consists of a number of techniques that are constantly evolving. It can be done remotely, but can also involve physical interference with a device or system - for example by forcing the unlocking of a mobile phone.

• It may also involve exploiting people to gain access to their technology. An example of 'phishing' is when an attacker impersonates a trusted person or organisation and sends a malware-infected link or attachment.

How can hacking be used in communication?

• Hackers can hack communications, for example by using 'IMSI catchers'. However, IMSI catchers can only intercept information transmitted between a mobile device and a base station; IMSI catchers cannot access information stored on the device.

• It can therefore use sophisticated hacking techniques to gain remote access to information stored on a phone, laptop or other internet-connected device, even if it is secured with a password, fingerprint or face lock.

• In addition, dropped, lost, etc. devices may fall into the hands of malicious people and access to them can be gained.

What should you pay attention to?

• Keeping your device up to date is a good way to prevent hacking, as hacking often takes advantage of vulnerabilities that have been disclosed but not yet patched.

• To increase your security and minimise the risk of being hacked, make sure your device is running the latest available version of the operating system (Android or iOS) and that all your apps are up-to-date.

• While you should keep your phone or other electronic devices locked, some hacking techniques can access even locked devices. However, the ability to bypass this security depends on the hacking technique used and the device it targets.

• Before travelling somewhere or connecting to a network where you feel unsafe, you may want to consider backing up your phone data to another device and then removing it from the devices you take with you. However, you should be aware that some hacking tools can recover deleted data. If you saved the data to a cloud service, some hacking tools can still access it.

• To avoid 'phishing' attacks, you should always be careful about which links you click on.

PHYSICAL SURVEILLANCE









BODY WORN CAMERAS

What do body worn video cameras do?

• Body Worn Video (BWV) cameras can be worn on a person's clothing - usually at chest, shoulder or head level, or on the collar - and record video, including audio, from the wearer's point of view.

• BWV cameras are likely to be visible to you and a flashing light should appear on the device when recording.

How can body cameras be used?

• BWV cameras can be used to closely monitor people's movements. There are cases of their use by law enforcement or private security during peaceful protests.

• Although the use of BWV camera recordings by individuals is illegal, in order for the BWV camera recordings used by the police to be in compliance with the law, the person whose image and voice will be recorded must be informed about the "image and voice recording" and what it will be used for.

• Secret BWV CCTV footage is illegal.

• The images can then be processed, for example, by facial recognition software.



A GUIDE TO PROTECTING YOUR VEHICLES AGAINST SURVEILLANCE



HOW TO BETTER CONTROL ACCESS TO YOUR LOCATION DATA

Where is my phone's location data stored?

The location of your phone can be determined in two main ways using GPS or mobile network location:

1. GPS

- GPS (stands for Global Positioning System) uses satellite navigation to locate your phone very precisely (within a few metres) and relies on a GPS chip inside your phone.

- Depending on the phone you use, your GPS location data may be stored locally and/or in a cloud service such as Google Cloud or iCloud. It may also be collected by any application you use that has access to your GPS location.

2. Mobile network location

- Mobile network location (or Global System for Mobile Communications (GSM) positioning) is based on your cellular network and can be determined as soon as you are connected to the network (i.e. when your phone is switched on and not in aeroplane mode), but is much less accurate than GPS. Your approximate location can be determined within an accuracy range of tens of metres in a city or hundreds of metres in rural areas.

- This location data is stored by your network provider.

Other methods can be used to indirectly determine your location, such as open wifi hotspots and Bluetooth beacons that your phones connect to, or location metadata embedded in your photos.

How can my location data be accessed?

There are several methods that other people can use to access the location (of your phone):

1. GPS

- Access to GPS location data depends on where the data is stored. It can be done using a 'mobile phone extraction' device that plugs into your phone and downloads all the data stored on your phone, including details of the places you have visited.

- Access to your GPS data may also be possible through device hacking, an advanced technique that does not require physical access to your phone and can be done remotely.

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

- Your GPS data can be accessed through your service provider.

2. Mobile network location

- Your approximate location data can be accessed through your service provider.

- Another way to access the same information is to use an 'IMSI catcher' (also known as a 'Stingray'), a device used to capture and track all mobile phones that are switched on in a given area and connected to a mobile network.

How can you better control your location data?

1. GPS

- The best way to prevent your location from being accessed is to limit the creation of location data in the first place

- In the case of GPS, this can be as simple as switching off your GPS (often referred to as 'location services'). Note, however, that location data from situations where you previously had GPS switched on may still be accessible.

- If you still need to use GPS on your phone, check individual apps' permissions to access your location to minimise the spread of this information.

- Removing permissions to access your location for all applications can prevent this data from being stored in an online account.

- If you absolutely need an app to access your GPS data, review the settings for that app to make sure you understand whether your location is stored online or only locally in your app. For example, if you use Google Maps while logged in to a Google account, you may want to disable location history in the settings so that your location history is not stored in your Google account.

- If you take a picture with your location services turned on, the location where the picture was taken may be included in the metadata (known as EXIF data) of the picture. You may want to disable location services when you take a photo, or you can use software or an app to delete this EXIF data later (for example, the Signal messaging app deletes EXIF data when you send an image).

- Similarly, by switching off your wifi or Bluetooth, you can prevent your phone from connecting to unwanted access points and providing indirect location information.

2. Mobile network location

- In the case of mobile network location, the only way to control this is to completely block connection to the network.

- If your phone is switched off, in aeroplane mode or in a faraday cage, it will block the connection to your mobile network and therefore make GSM geolocation impossible. A Faraday cage or switching off your phone prevents any type of connection to any telephone network. However, simply using aeroplane mode means that some types of connection can still be made (for example Bluetooth or GPS).

HOW TO ACCESS YOUR PHONE'S PICTURES, CONTACTS, DOCUMENTS AND HOW YOU CAN BETTER CONTROL YOUR PHONE



Where are my pictures, contacts and documents stored?

- You generate data every time you use your phone, for example when you take photos or record videos, create or edit notes and documents on the go, and add new names and numbers to your contacts.

- All this data is created through specialised apps - your camera and photo apps, social media apps, notes apps and contacts app are just a few examples.

- When you create any file on your phone, you will often also create 'metadata' attached to it (for example, a photo will have metadata such as the time and place it was taken). This metadata can be as descriptive as, if not more descriptive than, the photo itself.

- All this data will be stored on your phone's internal memory (including on any inserted external memory such as a MicroSD card) or in the Cloud, or both if you use any cloud service as a backup.

How can my images, contacts and documents be accessed?

There are several ways in which this data can be accessed, depending on how it is stored:

- If you store all your data locally on your phone, it can be accessed using a 'mobile phone extraction' device that connects to your phone and downloads all the data stored on it. This method cannot be used remotely - anyone wishing to access this data will need physical access to your phone.
- Device hacking is an advanced technique that gives you access to a certain amount of data on your phone, but not necessarily all of it. Unlike mobile phone extraction, device hacking does not require physical access to your device. This means that this method can be used at any time before or after a protest.
- If you synchronise your images, documents and contacts using any cloud service (e.g. iCloud, Dropbox or Google Drive), malicious actors may use remote 'cloud extraction' tools to access this information without your permission or knowledge or make a legal claim to the cloud service provider.

How can you limit the risk of your pictures, contacts and documents being accessed?

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

HOW YOUR DIGITAL COMMUNICATIONS CAN BE ACCESSED AND HOW YOU CAN BETTER CONTROL YOUR PHONE

Where are my communications stored?

- Text messages/phone calls:

Traditional mobile phone communication takes place over the cellular network. You access these via text messaging and phone call applications, which are usually provided as standard on your phone. While phone calls are not stored anywhere, text messages are stored locally on your and the recipient's devices. They can also be temporarily stored by the network provider.

- Social networks:

Except in rare cases of decentralised/self-hosted systems, your communications on social networking applications will be stored by the service providers.

- Messaging apps:

Messaging platforms provide highly secure communication over the internet. Depending on the application you use, your messages may be stored locally on your and the recipient's phone, on the service provider's systems and potentially online. Some messaging apps also offer backup solutions and these backups can be stored either online or locally. Different messaging apps are also based on different protocols, which means that some messaging apps are more at risk of eavesdropping than others.

How can my communications be accessed by other people?

There are several ways in which other people can access this data, depending on where you store it:

- Accessing communications stored on your phone (such as your conversations in a text messaging application) can be done through a 'mobile phone extraction' device that can be connected to your phone to download all the data stored on your phone.

- Such access may also be possible through device hacking, a technique that does not require physical access to your phone.

- If your communication is connected to a service provider or a social network (such as Messenger, Telegram, Instagram, TikTok), others may gain access through 'cloud extraction' technologies without your consent or knowledge. The same technique can be used to access backups of your communications (e.g. WhatsApp backups in Google Drive/iCloud).

- Your text messages and phone calls can be intercepted, recorded and intercepted by others using an 'IMSI catcher', a device used to monitor all mobile phones that are switched on and connected to the network in a given area.

- Your text messages may also be accessed through a legal process targeting your service provider. Similar legal processes can also be used to request data from companies that may host your communications (e.g. Twitter, Facebook).

- In addition, if there is an investigation in which you are a suspect, your accessible communication can be legally monitored by law enforcement officers with various technologies with a court-issued telecommunication surveillance decision. This surveillance will cover the period specified in the decision after the decision.

How can you limit the risk of your communications being accessed?

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

- Consider face-to-face contact when sharing highly sensitive information.
- 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 communication encrypted messaging apps to share sensitive information.
- However, if you use cloud backup for any of your messaging apps, be aware that the content can be accessed using cloud extraction tools.

VPN GUIDE



A GUIDE TO USING A VPN

In the world today, as governments and/or malicious individuals and organisations continue to exert control over access to the Web, including blocking websites from spying on people's online activities, people are increasingly turning to VPNs to access social media and online information.

We know that people turn to VPN as a precautionary measure to use the internet more freely or not to leave a digital footprint behind while surfing the internet.

What protections can VPNs offer?

- It adds an extra layer of encryption between your device and the VPN output, hiding the content and metadata of your traffic and the true destination of your internet browsing from your internet service provider (ISP).

- It hides your device's IP address from websites and apps by routing your traffic through a third country, which can bypass country-based blocks.

What are they not offering?

- It does not hide the existence of your phone from IMSI catchers.

- It does not protect against someone physically controlling the device, i.e. it does not hide the content on the device, including call and browsing history and messages.

- It does not hide the physical location of the device obtained from GPS or base station triangulation, i.e. it will not protect you unless you have taken other measures to hide your location, for example tagging your social media posts as location.

What is a VPN?

VPN, Virtual Private Network, routes your internet traffic through one or more servers, allowing it to access the wider internet.

VPNs are often used in business contexts to connect people physically located outside the office to internal services or to connect geographically separate sites to an intranet. Commercial VPNs are becoming increasingly popular in countries where access to social media and communication platforms is blocked, because they provide access to these websites if the VPN server is located outside the blocking country.

These commercial VPN servers are often located in other countries or even on other continents. As a result, they allow you to visit websites as if you were physically in the VPN server country.

What protections can VPNs offer?

- Adds an extra layer of encryption between your device and the VPN output, hiding the content and metadata of your traffic and the true destination of your internet browsing from your internet service provider (ISP).
- It hides your device's IP address from websites and apps by routing your traffic through a third country, which can bypass country-based blocks.

What are they not offering?

- It does not hide the existence of your phone from IMSI catchers.
- It does not protect against someone having physical control of the device, i.e. it does not hide content on the device itself, including search; browsing history and messages.
- It does not hide the physical location of the device obtained from GPS or base station triangulation, i.e. it will not protect you unless you have taken other measures to hide your location, for example geo-tagging your posts on Social Media.

Protection limitations of VPNs

- Commercial and free VPNs make many claims about "privacy" and "security", but there are limits to what they offer.
- In reality, you are changing who you trust to see the true source and destination of your Internet traffic, from your phone company, ISP or WiFi service to the VPN provider.
- VPN traffic has to access the internet from a server at some point, and these servers are available for observation by nation states and other malicious actors.
- Like all technology, VPNs can make mistakes. This can mean traffic not being routed, or certain types of traffic not being routed that could allow you to be detected by a sufficiently motivated attacker. You may not be aware of this error, meaning you could accidentally post on social media through your usual ISP or visit a website using your real IP address.

What should you look for when choosing a VPN?

- The jurisdiction of the VPN provider is very important. Look for VPNs located in countries with strong data protection and privacy laws.
- What the VPN demands of you - especially if it's free. Some VPNs allow others to use your device as the exit of their tunnel, meaning their traffic will appear to come from your device. For example, if another user engages in illegal activity, this could cause problems for you.
- There are other steps you can take, but none of them are perfect solutions.

Privacy International

62 Britton Street London EC1M 5UY United Kingdom

+44 (0)20 3422 4321

privacyinternational.org

Privacy International is a registered charity (1147471), and a company limited by guarantee registered in England and Wales (04354366).