حـملـة – المركـز العربـي
لـتطويـر الإعـلام الاجتماعـي
7amleh - The Arab Center for
the Advancement of Social Media

Guide to Digital Safety and Privacy at Peaceful Protests

December 2021

7amleh - The Arab Center for the Advancement of Social Media

Guide to Digital Safety and Privacy at Peaceful Protests

Lead researcher: Firas Taweel
Associate researcher: Buthayna Sifariny
Legal review by Abeer Baker
Translated by Ritaj for Managerial Solutions

This guide was produced in partnership with Privacy International as part of the adaptation of Privacy International's Free to Protest guide.

Important note: The information presented in this guide is not comprehensive and should not be construed as legally binding.

Contact us:
Email: info@7amleh.org
Website: www.7amleh.org
Telephone: +9720774020670
Find us on social media **7amleh**

Introduction

In recent years, there has been an increase in peaceful protests across the West Bank—including Jerusalem—the Gaza Strip, and Israel. Recent examples of this trend include, the protests against forced displacement of the Sheikh Jarrah neighborhood in Jerusalem, Mount Sobeih protests in the village of Beita in the West Bank against the illegal settlements, peaceful protests against police repression and homicide in Palestinian cities and villages across Israel, and the Great March of Return demonstrations in the Gaza Strip. As a result, violations against protesters have increased—including arrests and repression, in general, and digital violations, e.g., phone hacking, privacy violations, unauthorized access to digital information, and surveillance of freedom of expression, particularly online.

This guide is the fruition of our partnership with Privacy International, which developed a compendious guide to digital safety and privacy protection at peaceful protests over the past few years. For its part, 7amleh- The Arab Center for the Advancement of Social Media adapted the content and the design of the Privacy International’s *Free to Protest: The Protester‘s Guide to Police Surveillance and How to Avoid* it to fit the Palestinian context. To that end, 7amleh carried out field research, including five individual interviews with Palestinian journalists, activists, and human rights defenders who participated in peaceful protests in the West Bank—including Jerusalem—the Gaza Strip, and Israel over the past two years. In addition, it held three focus groups comprising journalists and activists in the West Bank—including Jerusalem—the Gaza Strip, and Israel—one group per represented region.
The guide is organized in three sub-guides: (1) a guide to digital safety and privacy at peaceful protests; (2) a guide to surveillance of protesters’ faces and bodies; and (3) a guide to policing databases and predictive policing tools.

The information presented in this guide is not comprehensive and should not be construed as legally binding.

The Palestinian
Observatory of Digital
Rights Violations
(7or)

The Palestinian Observatory of Digital Rights Violations (7or)

In the event of digital violations such as hacking, privacy violations, and surveillance of freedom of expression, 7amleh, through its 7or platform, extends the support by monitoring and documenting violations and following them up with the prism of social media companies, other relevant authorities, or both. You can visit the 7or platform through this link: **https://7or.7amleh.org**

Guide to Mobile Privacy at Peaceful Protests

What tools and techniques are used in the West Bank, the Gaza Strip, and Israel to surveil protesters' devices?

Confiscation and hacking:

In recent years, many protesters reported that their phones were confiscated during peaceful protests in the West Bank- including Jerusalem, the Gaza Strip, and Israel. It is common to target participants who raise their phones to photograph protests. Phones may also be confiscated if protesters are arrested.

In the case of direct access to handsets, relevant authorities often use mobile phone extraction (MPE) tools—software that allows their users to extract data from mobile phones without the consent of their owners and without the need to know the mobile passcode. The Israeli company Cellebrite stands as one of the most noted MPE software developers. A slew of governments around the world equip their police with such tools.

MPE techniques allow access to:

- contacts;
- call data (i.e., whom you call and when);
- text messages (including whom you texted and when);
- stored files (e.g., photos, videos, audio files, documents);
- app data (i.e., the apps installed on your device and the data stored on these apps);
- location information history;
- Wi-Fi network connections (which can reveal the locations of any place where you have connected to Wi-Fi);
- Some MPE tools may also access data stored in the cloud, or data you do not know exists or deleted data.
- It should be noted that MPE cannot be devised without direct access to the device, i.e., it cannot be processed remotely or over a wireless connection.

Points to consider about MPE when going to a protest—

- Keep your phone's operating system—whether Android or iOS—up to date, which means it will have the latest security features, is likely the best way to prevent MPE;
- Use a solid passcode to keep your device immune against MPE. Although some MPE tools are reported designed to access even locked phones, their ability to bypass this security does depend on the phone and its operating system;
- Most smartphones provide their users with a data backing feature to back up their mobile data and remove it from their phone. Of note, some MPE tools can recover deleted data.
- If some of your apps automatically save data (e.g., location data and messages) onto a cloud service, some MPE tools can still access the data even if the phone is locked. Specific MPE tools can access the data saved onto a cloud service, whether such data were directly saved by the user or automatically by apps. This includes messages exchanged via encrypted apps such as WhatsApp if the user enables the backup feature. Besides, this includes the location data history saved onto chatting or delivery apps.

Device location tracking

Over the past year, many *protesters reported receiving short text messages warning them not to be in protest areas. Such warnings were reported in the Gaza Strip (e.g., the Great March of Return), the West Bank (e.g., protests in Beita village), Jerusalem, and Israel.*

The device location can be tracked via the mobile SIM card directly through the data collected by the communication service provider—most notably International Mobile Subscriber Identity (IMSI) Catcher. This device locates any SIM card(s) connected to the device in a specific area by intercepting the data from that phone to the cell tower. Devices can also be tracked via the Global Positioning System (GPS). GPS uses satellite navigation to locate the user's phone via a chip inside the handset.

Points to consider about mobile location tracking when going to a protest—

- You may switch off your GPS manually at any time; If direct access to the device is available, hacking techniques can be used to access the location data history, including any location the user has been in previously, without turning off the GPS feature;
- Some applications store location data onto user's online accounts. These accounts can be hacked remotely without accessing the phone directly. You may turn off all apps' permissions to access your location manually. User data may not be stored online if the user use such apps as guests without creating accounts to use such apps;
- It is difficult for the software to track the phone if the flight mode is activated, the phone is turned off, or the Wi-Fi and Bluetooth features are disabled. However, the Airplane Mode does not necessarily disable the GPS and Bluetooth features;
- While phone signals, SMS, or logs of some chat apps can be intercepted, encrypted chat apps like Signal or Telegram offer higher privacy.

Social media monitoring

In recent years, tracking and monitoring social media have been one of the techniques with the most tangible impact on protesters in the West Bank—including Jerusalem, the Gaza Strip, and Israel. By scanning social media and collecting information and content published by or about specific people or events, storing and analyzing such data, and comparing it with previously stored data, authorities have what it takes to build files and records about people, groups, events, or all. With the prism of this data, they can better track activists, anticipate protests, and identify protesters. This, in many cases, may end in arresting people before, during, or after the protest—or thwarting protests and preventing them from happening.

How is social media monitoring used in relation to protests?

- Protest organizers will often use social media to organize protests, communicate with protesters, and upload photos and videos of protests; In turn, this means any party can 'data mine' social media posts to learn the identities and affiliations of the organizers and participants;
- Some participants post photos and videos of the protest after long periods. Whether old or related to a future event, all of these posts can be wielded to identify those present.
- Facial and gait technologies can be used to place people appearing in a specific photo or video.

Points to consider about social media monitoring when going to a protest—

- If you upload protest images or videos to your social media accounts, they may be used to identify and track individuals appearing in such photos and videos by using features as tagging or mentioning;
- If your location settings are switched on for your social media platforms or app(s) in use, and you then post online, some tracking and monitoring software can monitor any posts shared in specific time and place, e.g., the protest time and location;
- The camera app in most smartphones stores the image location data. Of note, this feature may be manually disabled via settings;
- Data such as the location, date, and time the photo was taken and the device used are stored in the EXIF information associated with the photo/video. EXIF data may be removed before posting any photo to social media platforms via the image properties.

Remote hacking

Hacking refers to finding vulnerabilities in electronic systems, either to report and repair them or to exploit them. An array of techniques can be used to hack handsets, including but not limited to remote manipulation of people to hit intrusive links (i.e., phishing attacks).

Points to consider about hacking when going to a protest—

- Keep your device operating system up to date—the more updated the version is, the higher the privacy and safety;
- In the same vein, the more updated the version of any app is, the higher protection and privacy would be whenever the app is used;
- Phishing is one of the most common ways to hack phones remotely. These links may appear as pop-ups, SMS messages, emails, etc. Such messages usually contain tempting offers designed to get users to click the link quickly. To name a few advertisements for financial prizes or mega contests. What is more, such messages are often sent through fake or hacked accounts, prompting recipients to click on links that they may receive from their friends and close acquaintances;
- The sender's identity can be verified via a particular app, or the seriousness of their message, by messaging them through another application.

Identity recognition through mobile 'unique identifiers'

Each phone has "unique identifiers" that may be used to identify their owners. The unique identifiers include the SIM card, the mobile user identity data, and the IMSI—a unique number associated with your SIM card. The latter does not change, even if the user puts the SIM card into a different phone. The IMSI is associated with personal information such as the username and address. Besides, there is the International Mobile Equipment Identity (IMEI)—another unique number identifying the phone (the device). So, if the user changes the phone, the IMEI will be changed. IMEI may include data about the username and address and the device model and brand. Unique identifiers may also include ad ID history. The phone operating system generates the ad Id to offer personalized ads for the user. Ad Id may be associated with the user's personal information (e.g., name, geolocation, websites visited). Ad ID may be scanned and updated manually via the mobile settings.

Points to consider about the phone unique identifiers when going to a protest—

- Switching off your mobile or set it in Airplane Mode may limit the ability of technologies to intercept the "chip" connection and access its data;
- Users can scan the data stored onto their mobile to feed the ad algorithm manually at any time; The user can also disable the personalized ads feature on the phone at large and on the apps and internet browsers they use; Users may use an ad blocker to better protect the privacy of their personal information

A Guide to Surveillance of Protesters' Faces and Bodies

What tools and techniques are used in the West Bank, the Gaza Strip, and Israel to surveil protesters' faces and bodies?

Facial and gait recognition technologies

Facial recognition technology (FRT) collects and processes data about people's faces and can identify people. FRT matches captured images with images stored in existing databases or 'watchlists'. For example, the Israeli authorities use CCTV cameras in occupied Palestinian territories—including Jerusalem and Israel to identify protesters. Surveillance and security cameras are widely deployed in Palestinian neighborhoods in Jerusalem, in the "seam" areas and military checkpoints across the West Bank, and on the separation fence on the northern Gaza Strip borders. These cameras are used to determine the identities of those present in those areas by comparing the captured images with ready-made watchlists containing facial data and/or fingerprints of Palestinians. Of note, many Palestinians provide their iris and fingerprint data annually to various authorities. For example, in the West Bank, Palestinians wishing to obtain a permit to work or visit Israel often must provide the authorities with an eye-and-fingerprint. In the same vein, in the Gaza Strip, many citizens provide such information to obtain the Qatari grant. These technologies may be devised to analyze live photos and videos as well as previously captured materials.

Points to consider about face and gait recognition technologies when going to a protest—

- Facial recognition technologies can distinguish people's identities by capturing a range of distinctive features of their faces. However, these technologies are usually less capable of identifying when they cannot identify facial features if people wear glasses, medical masks, or both;
- The police have the right to ask any citizen to remove any face covering, but these rules may change in the context of the Corona pandemic;
- Some photo and video

editing tools offer the ability to lower the quality of these materials and/or blur certain parts of them. Note that any photos or videos posted on social media or media sites are monitored by various authorities.

Protesters' gait recognition

In recent years, many Palestinian activists have reported that gait recognition technology (GRT) is used by different authorities, especially in Israel, and Jerusalem. GRT usually zeros in on the chest, shoulder, or head level. In the West Bank and the Gaza Strip, authorities may also use handheld cameras or mobile phone cameras. These cameras may be used to track participants' identities in peaceful protests, and they may be used by the police or security personnel in civilian clothes.

Points to consider about GRT when going to a protest—

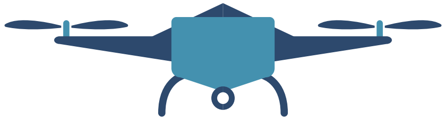
- Some jurisdictions consider GRT as a witness. Notwithstanding, the camera owner controls the operation and/or stopping of filming, which makes them able to control the content of the documentation. Also, cameras often do not document the actions of the camera owner;
- Facial identification techniques can be used to track the identities of those present in body camera recordings and others, which depend on collecting distinctive features of people's faces and bodies, and become less able to work in the absence of clear clips of those features;
- Any individual has the right to request the deletion of any photo or video in which they appear clearly, whether at the moment of capturing or after posting on the internet or in the media—even if it was taken in a public place.

Drones

In recent years, the use of drones by various authorities has escalated in protests in Palestine, especially in the Gaza Strip, in the Great March of Return, and protests and demonstrations in the West Bank, Jerusalem, and Israel. Drones can be equipped with regular cameras or cameras with FRT. The drone can also be equipped with IMSI tracking technologies to track specific phone chips.

Points to consider about drones when going to a protest—

- A drone's ability to track the identities of individuals depends on the type of aircraft—not all drones have the same capabilities;
- Facial technologies rely on clear segments of distinct features of people's faces and may be less effective if people wear sunglasses, medical masks, or both;
- Technologies to track the SIM card signal rely on intercepting its communication with signal towers. Therefore, if the phone is turned off or in Airplane Mode, these technologies may be less effective.



A Guide to Policing Databases and Predictive Policing Tools

Predictive police techniques rely on analyzing data on social media pages and in databases available to authorities (e.g., records of past incidents, security files, biometric data, facial identification data, and SIM card data) to predict or anticipate future "security events"—and accordingly justify arresting and/or summoning people for investigation.

According to several reports, the Israeli occupation authorities have been using predictive policing techniques extensively since 2015.

The authorities can use photos and videos from peaceful protests to feed these technologies, track the identities of participants, and/or include them on special lists. If a person is on one of these lists, they may be subject to arrest, interrogation, or detention and search in the future.

Often, the results of predictive police algorithms may be inaccurate and biased due to a gap in the data, which in some cases may lead to an intensification of violence in already vulnerable communities.

Points to consider about **predictive policing tools when going to a protest—**

Any photos or videos on social media platforms or CCTV recordings, especially those related to protests, can be used to feed predictive police databases;

Some users on social media platforms resort to encrypting "keywords" by using numbers, symbols, or letters from different languages to avoid being included on predictive policing lists.

The Palestinian
Observatory of Digital
Rights Violations
(7or)

The Palestinian Observatory of Digital Rights Violations (7or)

In the event of digital violations such as hacking, privacy violations, and surveillance of freedom of expression, 7amleh- The Arab Center for the Advancement of Social Media , through its 7or platform, extends the support by monitoring and documenting violations and following them up with the prism of social media companies and/or other relevant authorities. You can visit the 7or platform through this link: https://7or.7amleh.org www.7amleh.org

/7amleh