June 2022

حملة - المركز العربي لتطوير الإعلام الاجتماعي
7amleh - The Arab Center for the Advancement of Social Media

The Privacy and Personal Data File in Palestine...Dual Violations and Absented Law

Firas al Taweel and Buthaina Saffarini

The Public Prosecution, the Judiciary, and the Anti-Corruption Commission, are among multiple Palestinian official bodies that request information on subscribers of the telecommunications and Internet companies in the Palestinian Territory. While the Israeli Government controls the privacy of Palestinians through its policies, legislations, and dominance of its practices on Palestinian privacy, through hacking phones of employees of the Palestinian civil society organizations, and through its ability to track and surveille Palestinian communications and digital activity, as well as many other methods. As such, the Palestinian citizen is faced with dual challenges pertaining to the privacy and protection of personal data , under most prominently, the control of the Israeli occupation, and the absence of Palestinian laws for the provision of adequate and needed protection.

This report unlocks the privacy file and explores the extent of commitment of telecommunications, Internet providers, and electronic payment companies operating in the occupied Palestinian territory, to the policies pertaining to privacy and the protection of personal data; as well as the relationship between these companies and the Palestinian official bodies. The report elaborates further to highlight the extent to which

Palestinians are digitally and electronically exposed to the Israeli occupation.

Privacy, a Basic International and National Right

1. The right to privacy is not, by any means, a luxury, especially under the prevailing technology revolution. It rather constitutes one of the human rights stipulated in many international agreements and conventions. Article (12) of the Universal Declaration of Human Rights states: No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, or to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks." With a very similar text, Article (17) of the International Covenant on Civil and Political Rights states: “1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation; and 2) Everyone has the right to the protection of the law against such interference or attacks”. In addition to what is stipulated under Article (16) of the Convention on the Rights of the Child, and Article (14) of the United Nations Convention on the Protection of the Rights of All Migrant Workers.

   At the national level, the amended Palestinian Basic Law of 2003 explicitly states that human rights and fundamental freedoms are binding and respected under Article (10), which affirms that everyone in the State of Palestine, including the public authorities, their representatives, and employees, are legally obligated to respect human rights and fundamental freedoms, including the right to privacy and the sanctity of private/home life. Whereas, the Basic Law is at the top of the hierarchy of legal norms, all legislations shall be binding and shall not contradict or violate any of its provisions.

   Moreover, under Article (32), the Basic Law referred to the right to private life under the term: “the sanctity of private life”, as the article

states: “Each aggression committed against any personal freedom, against private life of human being, or against any of rights and freedoms guaranteed by the law or by this basic law, shall be considered as a crime. Criminal and civil cases resulting from such infringement shall not be subject to any statute of limitation, and the National Authority shall guarantee fair indemnity for those who suffered from such damages”.

In addition, the Basic Law explicitly states the protection of some components of the right to privacy, namely those related to the privacy of the body, and the privacy of the physical space occupied by the person “the sanctity of the home.” Article (11) stipulates that it is unlawful to arrest, search of any person except by a judicial order and in accordance with the provisions of the law; whereas, Article (16) of the law stipulates that it is unlawful to conduct any medical or scientific experiment on any person without securing the person’s consent and as provisioned by the Law. As for the privacy of the physical space, Article (17) stipulates homes as inviolable, thus, shall not be subject to surveillance, entrance or search, except in accordance with a valid judicial order and in accordance with the provisions of the law; it also stipulated any violations resulting of this article shall be considered invalid and nullified. Individuals who suffer from such violation shall be entitled to fair compensation by the State of Palestine.

Despite the fact that the Basic Law does not provide for a comprehensive protection for all elements of the right to privacy, including the privacy of personal data and information and issues related to advancements of the technology, the text of Articles (10 and 32) of the law are a robust constitutional basis for the protection of the right to privacy, according to Ammar Jamous,[1] a researcher at the Independent Commission for Human Rights (ICHR), in particular, if international

[1] Jamous, Ammar, Interview in Ramallah, March 2022.

standards and criteria pertaining to communications surveillance and other forms of interference with privacy were to be incorporated within national policies, laws and procedures. Furthermore, this will enable measures for all other cases of interference with privacy stipulated items under Articles (11), (16) and (17), provided a valid judicial order is issued and in accordance with the provisions of the law, as stated by Jamous.

Cybercrime legislation, a key to hacking and violating the right to privacy

The core problem, as viewed by the ICHR, is the legal act/text of the provisions of the Palestinian laws regulating cases of interference in the privacy, such as searching people, homes, electronic devices, and confiscation/seizure of correspondence and mail, which constitute a real threat to the right to privacy and the sanctity/privacy of home and private life. This is a result of waiving the condition of a valid judicial order to allow the search or confiscation; and only requires the search or seizure warrant issued by the Public Prosecution, the Attorney General or, accordingly by one of his assistants; a matter that make these laws inconsistent with Articles (11, 17) of the Basic Law that stipulate a valid judicial order to search people and homes and to imposing any other restrictions on the freedoms of people.

The provisions for seizure/confiscation of correspondence were applicable to electronic correspondence and communications that take place through the information technology means, until a decree-law was issued under the cybercrime law. This legislation, which embodied detailed provisions, regulated cases of interference on privacy through the seizure of electronic messages. At the same time, the retraction of the safeguards that were affirmed by Article (1/51) of the Code of Criminal Procedures; where legal texts provisioned therein give the power to seize electronic messages - and much more - to the Public Prosecution or by a delegated law enforcement officer; an authority that

was previously exclusive to the Public Prosecutor or one of his assistants.

In addition, the Decree-Law has given the Public Prosecution the authority for the seizure and inspection of electronic devices for an indefinite period. It also stipulated the authority of the Public Prosecution Department to authorize the judicial law enforcement officer or persons of expertise to directly access any of the means of information technology, inspect to access data and information, unconditioned of securing a valid judicial order. This too, clearly shows the retraction from the safeguards provisioned under the Code of Criminal Procedure.

The decree-law also stipulates the authority of the Public Prosecution to access devices, tools, means, data, electronic information, pass words, data related to flow of communications, its users, or subscriber's information related to cybercrime. It also gave the Public Prosecution the authority for the seizure of the entire information system or part of it and the meaning it contains. The decree-law did not specify the extent of and significance of the crime that calls for such a serious interference with privacy. It also failed to oblige the presence of the accused or concerned person during the search and seizure; whereas, as it stipulated the necessity to prepare lists of seized items to the extent possible, which gives the Public Prosecution the freedom to edit this list, as the act text did not provide any obligatory form.

Mahmoud al-Franji,[2] Coordinator of The Palestinian Human Rights Organizations Council (PHROC), believes a problematic issue concerning the powers granted by some legal articles to the security bodies pertaining to the interference in the civil life; for example, what was cited in Article (3) of Decree-Law No. 10 of 2018 on Cybercrime, which states: "1) A specialized cybercrime unit shall be established

[2] Al Franji, Mahmoud. Personal Interview, March 2022.

within the police agency and security forces, comprising officers vested with judicial duties. The Public Prosecution shall be responsible for providing judicial supervision over it, each in the area of his jurisdiction. 2) Regular courts and the Public Prosecution, in accordance with their jurisdictions, shall hear cybercrime cases."

According to al-Franji, the security forces are (Preventive Security, General Intelligence, Military Intelligence and the Civil Defense), who are designated law enforcement officers with judicial duties. Thus, the decree-law gives power to all agencies to establish specialized respective units under the name “Electronic Crime Unit”, and the Public Prosecution shall undertake judicial supervision over them, while it (the Prosecution) shall only supervise the police apparatus.

Al-Franji further adds that human rights organizations demand the establishment of only one unit for cybercrime within the police force, to be authorized only for follow up on complaints and issues related to cybercrime. As per legal norms and practice, the legal supervision over law enforcement officers is assigned only to the Public Prosecution, while the Military Prosecution shall be responsible for the supervision of other security forces, the Preventive Security, Intelligence and National Security. This prompted al-Franji to ask: Are we going to deal with the police, or preventive security and intelligence? What about violators from the other security forces, will they be subject to the supervision of Civil or Military Public Prosecution?

This was evident in the incidents that followed the murder of activist Nizar Banat in June 2021, along with the abduction of female journalists and others in the field, whose mobile devices were snatched and assaulted. Accordingly, “Al-Haq”, along with 31 civil society organizations, filed a penal case/order in this respect to the Public Prosecution, in which the names were specified. Upon follow up on the issue, the response was that such issues are not within the jurisdiction of

the Public Prosecution, given that those whose names were mentioned were not security personnel, they are governed by the Military Prosecution, and accordingly, the file has been referred to them.

Legislations violated without prosecution or accountability... Activists are at risk!

The conflict/contradiction between the legal text and actual practice appears in the text of Article (22) of the Cybercrime decree-law whereas, “1) Arbitrary or illegal interference with the privacy of any person or the affairs of his family, home or correspondence shall be prohibited. 2) Each person who creates an electronic website, application or account or disseminates information on the web or any of the means of information technology with the intention of sharing and circulating live or recorded news, images, audio or visual recordings, is considered illegal interference with the private or family life of individuals, even if they were true, shall be punished by either or both confinement for a term of not less than one years and a fine of not less than one thousand Jordanian dinars and does not exceed three thousand Jordanian dinars or its equivalent in the legal currency of circulation, or both penalties”.

However, what took place in reality, during the popular protests that followed the assassination of the political activist Nizar Banat by members of the Preventive Security Service during his arrest on June 24, 2021, with a number of female journalists, contradictedto Article (22). Over the course of three days, these protests were subjected to repression; however, the most serious incidents of repression that the city witnessed was on June 27, 2021, when security forces in civilian clothes attacked the demonstrators at the al Saa’a Square in the city of Ramallah. The day also witnessed the theft of the mobiles of demonstrators and journalists, on a large scale, and in particular, the theft of the phones of female journalists and demonstrators.

At a later date, some very private/personal photos of female journalists and demonstrators that were saved in their stolen mobile phones, were posted and circulated to groups of the WhatsApp application and on Facebook pages. Moreover, some of these female journalists and demonstrators were subjected to blackmail and threats to discourage them from taking part in protests or covering them. Human rights organizations considered these acts as serious violations of human rights, including the right to privacy, in addition on exploiting gender dimensions under the prevailing cultural and social restrictions, the embarrassment and fear for the harming the reputation and defamation, which reflect on increasing the suffering and anxiety of victims preventing them from seeking judicial redress.[3]

On 1st July 2021, a group of institutions submitted a complaint to the Public Prosecutor to prosecute those involved; the Public Prosecution informed of its referral to the Ministry of Interior to pursue necessary investigation and assembling of evidence to identify the suspects. According to Nasser Jarrar,[4] Head of the Cybercrime Prosecution, the total number of complaints received by the Public Prosecution and the police related to the incidents of June 27 was only 4-5. Jarrar also informed of the referral of a file of a security officer proven to have used the phone of one of the female demonstrators to the Military Prosecution; he added that Public Prosecution did not reach any conclusions or findings with respect to the other complaints. Jarrar called upon all harmed and subjected to violations to file complaints, saying,

[3] After these incidents, a campaign was launched to combat posting pictures of girls whom mobiles were stolen on social media platforms; Sada Social Monitor affirmed that Facebook has responded positively to their request for the closure of pages that conduct misleading actions:

https://www.facebook.com/SadaSocialPs/photos/a.160803707592257 4/4303721846354070/?type=3.

[4] Jarrar, Naser, Personal Interview.

"The majority of those who spoke about violations did not file complaints, and the actual number of received complaints is few."

Despite the procedures indicated by the Public Prosecution Office, and despite the pursuance by the Military Prosecution of the officers accused of stealing and selling the phone of one of the female protesters, however, the limitation of accountability procedures adopted remained vivid. A matter that requires bodies of Law Enforcement, headed by the Public Prosecution, take serious measures to pursue those involved in the assault of demonstrators and the theft of their phones in order to bring them to trial, as demanded by the ICHR.

Najla Zaitoun, [5] one of the journalists who reported the confiscation of her phone during the security forces' oppression of the protests in Ramallah. After 3 days of filing a complaint, she learnt that she had more than one account in her name with pictures on both Instagram and Facebook platforms, and these accounts communicate with people using her identity/name. This drew the attention of the people whom these fake accounts contacted, where they saw Najla's personal pictures posted and that she was following several pornographic sites; in addition to seeing a story posted that shows Najla "desperate and thinking of suicide"; this was very worrying to her.

Najla reported the matter to people at the Cybercrime Prosecution who informed her that they do not have the capacity/ability to track the account; they added, "in case this is repeated she can bring the issue to their attention and report it again." Recently (in February), Najla received a "screenshot" from some of her acquaintances of an account that has her name and picture; to her, the fact that this fake account communicates using her name is worrying and disturbing.

[5] Zaitoun, Najla, Personal Interview, March 2022.

Moreover, Najla submitted an official complaint to the Military Judiciary pertaining to the confiscation of her mobile device, the hacking and violations of her privacy, however, after 3 days, she stopped following up on the complaint due to being subjected to blackmail through fake electronic accounts; and the lack of confidence in the judiciary and ability to protect her.

Transparency and Digital Security under the Grip of the Telecommunications Companies and Official Bodies

Ammar Jamous, a researcher at the Independent Commission for Human Rights (ICHR), believes that the Palestinian telecommunications and Internet companies lack transparency pertaining to the file on subscribers' privacy and their personal data. Similarly, and to the same extent, transparency appears to be absent in governmental and official bodies in Palestine. In his view, "the privacy policy adopted by the companies is not serious." He added, "We do not know the actual resources and technical and substantive capacities available to companies and various security agencies, furthermore, we do not know to what extent they can go in the tracking and surveillance of citizens' communications."

Video - Ammar Jamous

In an incident surfaced in February 2018, the former Chief of Palestinian intelligence, Tawfiq al-Tirawi, and the head of the Palestinian Bar Association in the West Bank, Jawad Obeidat, filed a lawsuit against the Palestinian Authority (PA) and "Jawwal" Telecommunications Company claiming that the Authority had spied on them. The lawsuit was submitted after the circulation of a document on social media platforms; the persons who posted the document allegedly claim that it was leaked by the Authority; the document is of 37 pages and contains photos, personal information and transcription of phone calls attributed to them.

Obeidat told the “Associated Press”, at the time, that the transcriptions of his phone conversations are correct as stated in the document.

As for al-Tirawi, he stated that he checked his call log and contacts and believes that the posted document is correct. Meanwhile, Major General Adnan al-Dumairi, the official spokesperson for the Palestinian security services at the time, rejected the allegations and described the document as "nonsense.” Other informed resources, familiar with al-Tirawi's complaint, said "the Prosecution examined the complaint at the time and did not reach any findings to prove the wiretapping hypothesis," however, they added, "The Prosecution did not close the file at that time." [6]

Among the incidents that raised the suspicion of the ICHR, according to Jamous, was what Facebook announced on April 21, 2021, that its security team, Threat interception Division, disrupted two separate hacking groups targeting users of the platform; one is linked to the Palestinian Preventive Security in the West Bank, and the other is a group linked to the well-known espionage outfit known as “Arid Viper”. These activities targeted opposition actors, civilians, journalists, legal personnel, and Palestinian officials and Arabs inside and outside the occupied territories, in the State of Palestine; Civilians, military officers, and members of the Fatah movement. The two groups relied on social engineering technology to access users’ data and information.

As a result, the ICHR demanded the government to investigate the findings and information reflected in the statement made by Facebook;[7] However, no information is available on the government taking any

[6] The New Arab (Al-Araby Al-Jadeed), “.Palestinian Lawyers: I accuse the authorities that are supposed to protect us of spying on our phone conversations”, February 5, 2018, https://www.alaraby.co.uk.

[7] The Independent Commission for Human Rights, “the Independent Commissions demands the government and the General Attorney to conduct a transparent investigation on facts reflected in the statement made by Facebook on the internet piracy in Palestine”, April 22, 2021, https://www.ichr.ps/media-center/3809.html.

investigative measures in this context; furthermore, no official information was furnished on government activities in the area of communication surveillance or the assembling users' data and information.

On the other hand, the "Lawyers for Justice"[8] group warned of the danger of some Palestinian Security Services forcing detainees to open their phones and browse their accounts without a legal warrant; the group confirmed that such cases were documented during conducting investigation with activists of the "Enough, telecommunication companies" movement.

Ongoing Complaints about Lack of Transparency, Hacking, and Personal Data Sharing

Over the past years, the ICHR has received hundreds of complaints from citizens about illegal interference with their privacy through the search/inspections (personal, home, and electronic devices) without a valid legal warrant issued by the Public Prosecution to authorize the search/inspection. The number of these complaints reached (45) complaints in 2021, (56) complaints in 2020, (49) complaints in 2019; while in 2018, it reached (58) complaints and in 2017 to (72) complaints. It was distributed as illustrated in the table below.

Year	Total	West Bank	Gaza
2017	72	35	37
2018	58	28	30

[8] Lawyers for Justice, Personal Interview, February 2022.

2019	65	22	43
2020	56	36	20
2021	45	28	17

Table: Number of complaints received by the ICHR over the past years on violation of the privacy of citizens during arbitrary and illegal search and inspections.

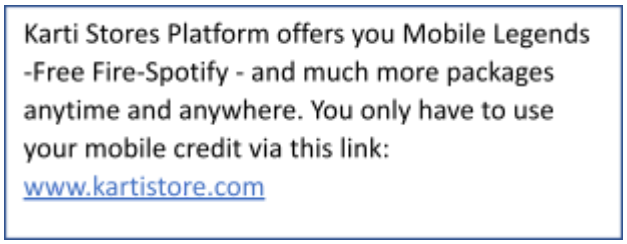
The Palestinian Monitor for Digital Rights Violations (7or), affiliated with 7amleh - the Arab Center for the Advancement of Social Media, documented (1121) violations of Palestinian digital rights; From the beginning of 2021 until January 2022, it included various violations; Of these, 17 cases of digital hacking.

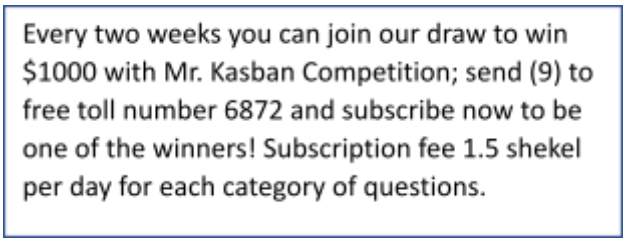
There are also communal queries and suspicions regarding the use of personal data such as subscriber's numbers, for commercial purposes. Izzedin Zaool, a Palestinian citizen and an activist in the "Enough, Telecommunication companies" movement, reported that more than one message from various parties, such as "Mr. Kassban" and "Karti", were received through his personal mobile! He wonders how these entities had his number. [9]

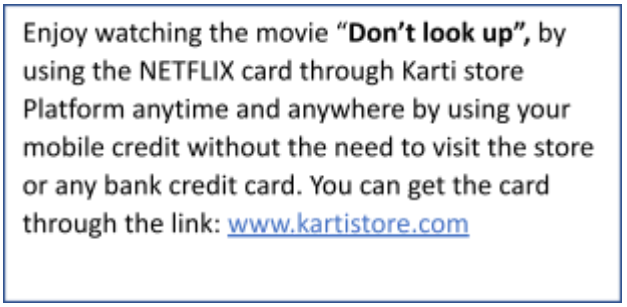
He was also surprised how Hadara Company managed to get his mobile number the minute he visited the Palestinian Telecommunications Company (Paltel) to apply for a landline phone connection, especially since Hadara is the arm of the Paltel Group for the provision of internet services to citizens. It became evident to him that his number and personal information were being "leaked" to the company to bombard him with packages and offers, "Otherwise, how would they get my number?" he questioned.

[9] Zaool, Izzeldin, Personal Interview. February 2022.

Zaool considered that as an infringement of privacy: “what right allow furnishing Hadara with my phone number, or to any other company?”







Video: Zaool

Cathrine Abuamsha, Local Advocacy Manager at 7amleh - the Arab Center for the Advancement of Social Media, says that in light of the apparent shortcomings in addressing the privacy and protection rights from a human rights perspective, in addition to the absence of an understanding of the right to privacy and data that must be protected, it is the state's duty to obligate internet providers and communication companies, as well as all other parties that have access to users' data whether directly or indirectly, to have a clear and binding policy in processing and protecting the right to privacy and right to protect the personal data of users.

Furthermore, Abuamsha elaborates by adding that the State of Palestine has acceded to International Human Right Conventions since 2014 which requires it to fulfill obligations, including the drafting and laws and administrative bylaws towards protecting privacy and personal data as well as regulate this file.

In addition, al-Franji discussed the issue pertaining to absence of transparency and lack of standards for the processing and circulation of personal data among the official sector and service providers, in particular the renewal of what is basically a “monopoly contract” for the Palestinian Telecommunications Companies which was signed during the term of Dr. Rami al-Hamdallah’s government; the text of the agreement is still not published until this day, which raises questions regarding whether it was in line with provisions of the law, the boundaries between the company and the government, and the granting of concessions or obligations of the company in exchange of the monopoly contract, in addition to the government’s conditions in exchange for signing the contract. Over the course of 3 years, demands have been made by "Aman" - The Coalition for Accountability and Integrity, and other civil society organizations requesting the government or the Ministry of Finance to provide a copy of the agreement in vain.

The copy is still not made available or reviewed. In 2017, the ICHR, Aman, and the and the Palestinian Society for Consumer Protection, called on government to publish the text for the renewal license agreement, to the Palestine Telecommunications Company - (Paltel) for the fixed networks, and Palestine Cellular Communications Ltd. (Jawwal), for the next 20 years as of November 16, 2016, at a value of (290) million dollars and all annexes related to it; such demands were substantiated by the citizens right to be informed; yet, until this day of 2022, such societal demands are still unanswered.[10]

2021: The Public Prosecutor's Office requested Data from the companies on 26 thousand occasions.

The Public Prosecution Office constantly receives requests from various security agencies (Preventive Security and General Intelligence in particular) to access information concerning subscribers under various investigative cases. All such requests are supported by a letter explaining the reasons and attached to the investigation file (evidence report). The Public Prosecution Office studies the requests and, forwards them to the relevant telecommunications companies; the later shall in response, provide the requested information pertaining to the persons involved in the investigative cases; in most cases, this information is often statements of the accused person's communications record (incoming and outgoing calls); however, the record does not include audio recording. According to Nasser Jarrar, head of the Cybercrime Prosecution- Public Prosecution Office, content of calls and text messages cannot be accessed and requires special techniques that are not available with service provider companies; He further reiterated that

[10] Aman, the "Independent Commission", "Aman" and the "Consumer Protection" demand the Prime Minister to promulgate the renewal of licenses agreement for to the benefit of (Paltel) and (Jawwal)". Aman, December 25, 2017. https://cutt.us/v0hXQ.

"the prosecution does not consider audio recordings, given they are illegal."

As for the mechanism for submitting a request to the companies, Jarrar informs of specific focal points within companies that can be contacted; requests are forwarded to these focal points/commissioners, assigned by the Attorney General. The same process is adopted with Internet providers, as they are asked for an "IP" to track the name of a person against whom a complaint has been filed. He added: We have technical capabilities through experts and engineers in the Cybercrime Unit (who enjoy the status of judicial law enforcement officers) to collect the necessary information and evidence. In the same manner, communication is carried out with the five electronic payment companies operating in the State of Palestine in accordance with directions of the Palestinian Monetary Authority.

As for the requests submitted by the Public Prosecution to telecommunications and Internet companies during 2021, the number has reached 26,000, and in 2020 it was 21,000. The companies cannot refute, according to Jarrar. However, he informed that his Prosecution rejected requests for data submitted by the security agencies on the ground of lack of evidence, and unconvincing; when asked about the numbers, he stated that: "The percentage is very small."

Nasser Jarrar video

Subscriber information… the Anti-Corruption Commission use of powers

In addition to the Public Prosecution and the competent courts, we found that the Anti-Corruption Commission was requesting from telecom companies (Paltel, Jawwal, and Ooredoo) data about subscribers in

investigative cases. The Commission based its requests on the text (Article 9, paragraph 4) in the amended Anti-Corruption Authority Law (No. 1 of 2005): It is the authority of the Anti-Corruption Commission to request any files, data, papers, documents or information, view them, or obtain copies of them from the entity that holds them, including the bodies that consider all of this to be confidential circulation in accordance with the legal procedures in force.

The head of the Cybercrime Prosecution says that the Public Prosecution learned that the former head of the Anti-Corruption Commission, Ahmed Barak - who took over the presidency of the Commission between 2019 and 2021 - requested from service providers information about subscribers, based on a text received in accordance with the anti-corruption law. Jarrar explains that the Public Prosecution conducted a legal study that concluded that “the Anti-Corruption Commission has no authority to request this, and companies have been prevented from providing them with any information, except through the competent prosecution or court as a guarantee of the confidentiality of subscribers and not to use this authority for personal purposes,” and continued; “Ahmed Barak was able to request and obtain this information from service providers for a short period, and was even using the matter to obtain contact information for employees of the Anti-Corruption Commission as well. Public Prosecutor Akram al-Khatib issued a decree banning companies from providing any official or party with information except through the prosecution or the court, according to Jarrar, and the Paltel Group confirmed it.

However, this behavior (requesting information) was followed before Ahmed Barak's arrival to the presidency of the Commission, according to what a private source said. “The Commission was asking companies for information about the communications of defendants in corruption cases

under the aforementioned article of the Anti-Corruption Commission Law," confirms the source, who requested anonymity.

What was the response of Paltel Group?

Paltel Group (Paltel Jawwal and Hadara – then), responded to queries pertaining to protection of privacy and personal data of subscribers, by stating that data of subscribers is of utmost importance , through following a series of procedures and criteria to guarantee privacy of subscribers and confidentiality of their data.

The Group's written response reiterated their keen commitment to apply international criteria and standards adopted to this effect; some of the most significant criteria adopted are the non-disclosure of any data of their subscribers unless to the concerned juridical entities in accordance with the Law; maintaining and archiving electronic log in for the staff to log on into different systems; conducting periodic review for the granted authority for staff based on the nature of their work.

Whereas, Ooredoo declined to respond to any of our questions on how they tackle subscribers' privacy and personal data protection issues.

Document- Image of Paltel Group email response with the full text

The Illusion of accountability continues in the absence of the Law and an independent regulatory body.

The local advocacy manager of 7amleh - the Arab Center for the Advancement of Social Media, Cathrine Abuamsha, indicated that privacy and the protection of personal data cannot be left to the decision and desire of companies and public authorities or to rely on proposed good intent, these are citizens' rights and they are the ones who own it. Thus, laws should be endorsed to regulate the protection of the right to privacy to include the processing of personal data; this has to be expedited in a prompt and correct constitutional manner, and in

accordance with the principles of human rights. In parallel, an independent observatory entity should be established to protect and regulate privacy", failing to do that, violations cannot be tracked, stopped or even mitigated, otherwise we will still witness and observe lack of accountability once committed". The issue will not end here, since in essence it is related to drafting frameworks that bind everyone to protecting Palestinians and their personal data, even in their dealings with non-Palestinian entities, which would contribute to limit the abuse and utilization of such huge quantity of information and data that can be accessed and cause significant harm, by the Israeli occupation, as stated by Abuamsha.

She also reiterated the importance of enhancing audience awareness on the concept and content of the right to privacy and personal data, given that lack of awareness of our rights can lead to facilitating breach. To this effect, the state should dedicate programs and mechanisms to raise awareness pertaining to privacy to individuals and their relationship with commercial companies, and official institutions.

The ICHR agrees with "7amleh" on the need to establish an independent national regulatory body to promote and enhance the right to privacy, assigned with the responsibility of securing and guaranteeing transparency and accountability pertaining to all official interventions in privacy, the sanctity of personal life, especially with respect to surveillance of telecommunication. This body/entity should be furnished with adequate financial and human resources and granting it with strong legal authorities to enable it to access all information and governmental procedures relevant to privacy.

Furthermore, the ICHR put a recommendation towards amending the decree-law pertaining to Cybercrime to attain legislative harmony with the Basic Law and the international Law on human rights, and towards

provision of maximum protection for the right to privacy and sanctity of personal life.

In light of this complex situation, Mahmoud El Efranji believes that enforcement of a law for the protection of personal data will furnish tools and mechanisms for accountability in the event of violation by security forces and will ensure fairness.

Whereas, at the official front, the legal advisor at the Ministry of Communication and Information Technology, Mariam Taweel, affirms the need to draft a law on the protection of data and privacy,[11] not only to govern the communication sector but for protecting data in general, for example, texts reflected in the amended Basic Law and in cybercrime decree-law are of general nature, leaving each sector to regulate the scope within its specialty in the absence of a unified law to protect all data in all sectors.

To address this, the Council of Ministers passed a decree in April 2016 for the establishment of a ministerial committee of a number of ministries to draft a law proposal for the protection of personal data, "which is still at the preparation stage, and will aim at regulating the protection of personal data and privacy in all sectors; endorsement of this law is of high importance due to the accelerating interest of the issue as well as multiple parties collecting the data in order to establish balance between the collection, provision and protection of data"

Privacy Policies of Internet Companies are Optional

According to Mariam Taweel, there is not, at the moment, any existing Law that oblige Internet providers in the State of Palestine to develop or adopt a policy for privacy; these companies are obliged to protect data in light of the license awarded by the Ministry; however, they are not obliged to put in place their own specific written policy, furthermore, the

[11] Taweel, Marim, Personal Interview. February 2022

companies do not expect to obtain Ministry's approval of the respective written privacy policy. This of course resulted in, as stated in a previous report prepared by Access Now and Impact International on privacy policies questioning (7) Internet providers in Palestine, namely, Hadara, Mada, Bnet, Fusion, Call You, Super link, and Zaytona" on legal liability related to subscribers' data protection; all responded with No, which translates to liability waiver by companies in the case of hacking, processing of data, or violation of subscribers' privacy.

"None of these companies mentioned or referred to its legal liability in case of misuse of the personal data of the client, whether the misuse attempted by the company or a third party of whom the company shares the client personal data with."

Moreover, "Super Link" strip the client from the right of pursuing any legal action or file legal case based on the following article: confidentiality of information under this regulation is the sole responsibility of the subscriber, who under no condition shall have the right to file a case/ pursue legal action against Superlink for Telecommunication and Internet services.[12]

The report concluded that all companies do not commit to criteria pertaining to the protection of data. It also draws the attention to the fact that a third of users are ignorant or lack the understanding of what is meant by privacy policy, and the other third do not even read the privacy policy when they use or subscribe to the Internet. Most subscribers do not even know how companies handle their information and data.

The Occupation…Full Control over Communication and Privacy

The Israeli occupation controls the infrastructure of the Internet and information technology of the Palestinians, in addition to owning state of

[12] Jaber, Nasma, Fatfta, Marwa, Samaro Dima, Access Now, Impact International for Human Rights Policies, "Violated/Lawlessness Privacies: handling and treatment of internet providers in Palestine of subscribers' personal information. August 2021. https://cutt.us/aHgBs.

the art and the most advanced technologies used for continuous and random surveillance of Palestinians and violating their privacy rights and statuary of their personal lives. This indicates - as supported by factual events - that Israel violates and exposes the privacy of Palestinians.[13]

In mid-November 2021, a soldier who works with Unit 8200 of the Israeli army, the unit responsible for electronic/cyber spying/espionage, said in an interview with Middle East Eye site, of routine Israeli breaches and hacking of Palestinian citizens privacy especially in the Gaza Strip, he further confirmed that Israel can tab in and listen to all phone conversation in both the West Bank and Gaza Strip.[14]

In November 2021, an investigative report conducted by Front Line Defenders, exposed that Israel hacked the phones of managers and staff of organizations of the Palestinian civil society, through the "Pegasus" application manufactured by NSO, the Israeli company. One of the persons subjected to such breach is Ubai al-Aboudi, Executive Director of "Bisan" Center for Research and Development, this hack was revealed after a short period of Israel's declaring six Palestinian civil society organizations as terror organizations denouncing their legitimacy. [15]

---

[13] For more information on the Israeli Occupation violation of Palestinians' digital rights including right to privacy, refer to: 7amleh – the Arab Center for the Advancement of Social Media, freedom of the internet in Palestine: Survey on violations and threats of digital rights, 2018.

https://7amleh.org/wp-content/uploads/2018/01/7amleh_Internet_Freedoms_in_Palestine_WEB_ARABIC-final.pdf

[14] For more information, refer to: 7amleh – the Arab Center for the Advancement Social Media, "Legal Institutions condemn usage of Pegasus Software to spy on Palestinian Activists", November 10, 2021.

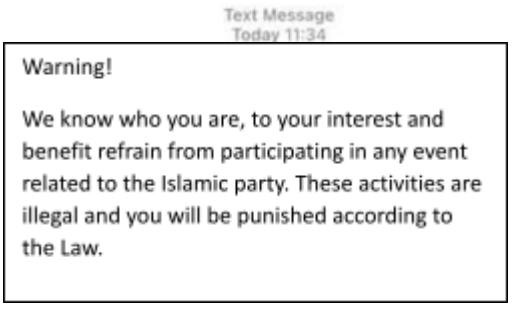
https://7amleh.org/2021/11/10/mussat-hqwqyh-tstnkr-astkhdam-brnamj-byjasws-lltjss-ala-nshtaa-flstynyyn .

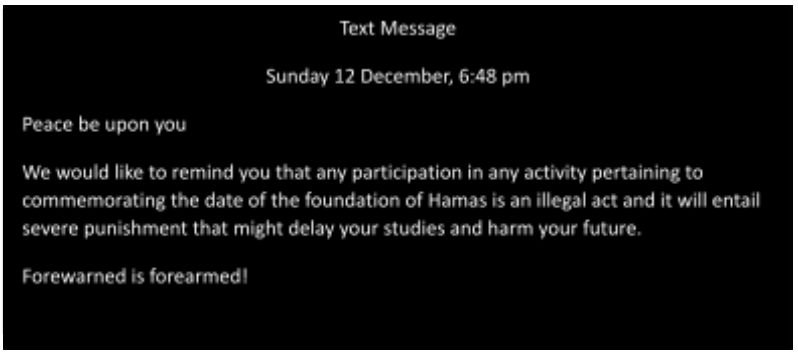
[15] For more information, refer to: Middle East Eye " Israel can monitor every telephone call in West Bank and Gaza, says intelligence source", November 15, 2021.https://www.middleeasteye.net/news/israel-can-monitor-every-telephone-call-west-bank-and-gaza-intelligence-source.

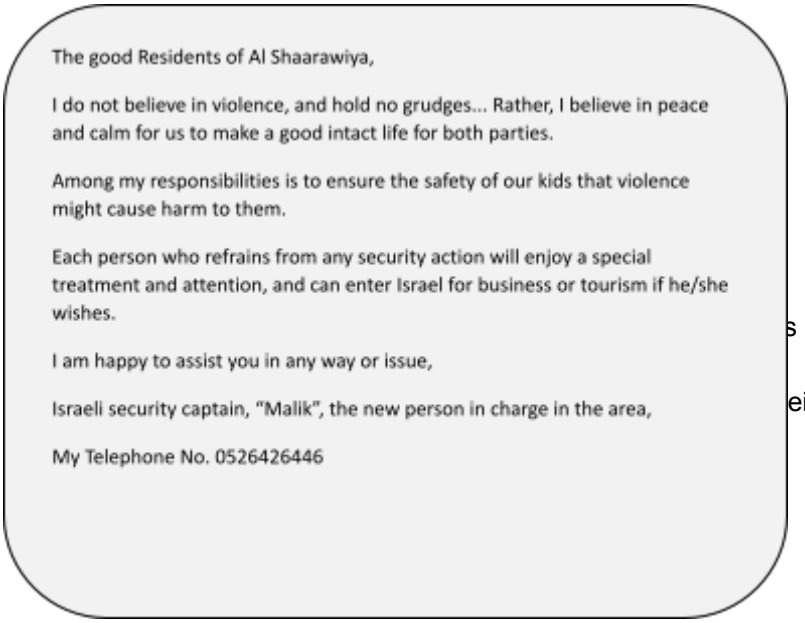
These breaches were firstly revealed, based on our talk with Ubai al-Aboudi,[16] when the call log of one of Al-Haq staff's mobiles listed calls that he did not conduct, his phone did not show any records of such outgoing calls in the log, while the log of outgoing calls for other persons listed such calls, al-Aboudi added, that any evidence based on such acts are rejected given that the person is targeted by such software.

Other examples of breaching privacy by the occupation, are the warning messages sent to the mobile phones of a number of students at the Birzeit University on January 12, 2021, discouraging them from taking part in any activities pertaining to commemorating the anniversary of the establishment of the "Hamas" movement.[17]

We have contacted one of the students at the Birzeit University who forwarded the text of the warning message, in addition to a message sent by the occupation not addressed to students of "Birzeit"





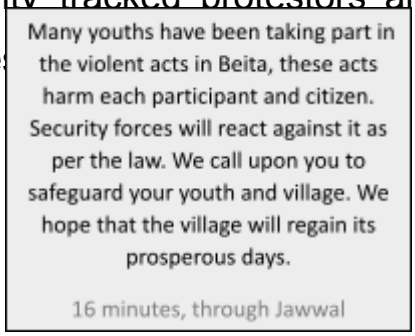


s of Birzeit University students after

eit University students after receiving


سكان الشعراوية الكرام,
أنا لا أؤمن بالعنف ولا أحمل حقد, بل أؤمن بالسلام والهدوء وكل هذا من أجل أن نقيم حياة سليمة وجيدة للطرفين.
من ضمن مسؤولياتي الحفاظ على سلامة أولادنا التي قد يتسبب العنف في اذيتهم.
إن كل من يبتعد عن أي نشاط امني يضمن معاملة مميزة واهتمام وأيضا يستطيع الدخول الى إسرائيل لعمل أو سياحة في حال أنه أراد.
أسعد جدا ان أساعدكم بأي موضوع, كابتن المخابرات الإسرائيلية "مالك" المسؤول الجديد في المنطقة. رقم هاتفي 0526426446

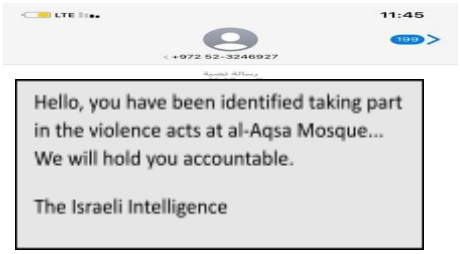
Similar messages have been forwarded by the occupation to the persons who took part in the protest demonstrations of “Jabal Subaih” in Beita village in Nablus. Journalist Mujahed Bani Mefleh stated that the occupation security tracked protestors and journalists and sent those warning messages[18]

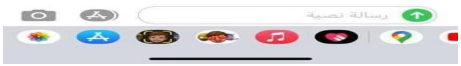

Many youths have been taking part in the violent acts in Beita, these acts harm each participant and citizen. Security forces will react against it as per the law. We call upon you to safeguard your youth and village. We hope that the village will regain its prosperous days.

16 minutes, through Jawwal

The same happened to persons present at al-Aqsa Mosque, as indicated by the youth Iyad Abu Saninah from Jerusalem.

[18] Bani Mefleh, Mujahed, Personal Interview, October 2021. https://cutt.us/NTblB .





The examples show the complex reality Palestinians endure in terms of privacy and protection of data under the Israeli occupation, the occupation prohibits Palestinian telecommunication companies from the provision of services in areas “C” with an estimated area of 60% of West bank land; Israeli companies illegally acquire 20-40% of the market share of Palestinian telecommunication market; this is done through sales of Israeli of Sim cards, exploiting and abusing the ban on Palestinian companies in area “C”, according to the fact sheet published by “Masarat” center on Israeli violations of digital rights.[19]

The paper also elaborated on an “important” point related to compelling Palestinian workers to download “Al Munaseq/Coordinator application” on their mobiles “, with the justification of providing information on work permits and lifting the security ban”; Upon downloading, the application requires access to geographical location, mobile files and data, camera, and any other information to the benefit of Israeli security and its coverage”.[20]

Another study mentioned the means the occupation utilize to access and collect personal data of Palestinians, for example, the army has installed temporary checkpoints in the west bank where they stopped men and demanded they fill a survey to include name, age, phone number,

[19] Hamda, Basel; Abed, Fadi. Arab Center for Policy Research and Strategic Studies – Masarat, “Facts sheet: Israeli Violations of Digital Rights”, September 2020. https://cutt.us/7xwSB
[20] Ibid.

identity card and license number, in addition to enclosing a copy of their Identification card. The survey included a question on the guarantees a Palestinian Law for the protection of personal data could provide and entail; response was “not as much”, therefore, even if the PA were to endorse a law for the protection of data, it will only provide a limited level of protection due to the full control of Israeli occupation over the Palestinian information technology and telecommunication infrastructure which has been maintained by Israel since its occupation of the Palestinian land in 1967.

During the signing of the “Oslo” Accord in 1995, the occupation handed over partial control over the information technology and telecommunication in the West Bank and Gaza to the PA; despite the fact that the agreement grants the PA the right to develop their own information technology and telecommunication, yet, “the Israeli authorities still fully controls, all electromagnet waves, in addition to the control of importing and installing any equipment by the Palestinian telecommunication companies and internet providers under the grounds of undeclared “security reasons”.[21]

To conclude, it is evident how the Palestinian right to privacy and the protection of personal data is subjected to negligence and exploitation; furthermore, their data is treated as “communal”, that are drained and breached by the occupation when and by any means it wishes. As opposed to this, and at the local front, the Palestinian Authourity failed to fulfill its commitments towards the privacy of Palestinians; despite the fact that the State of Palestine has acceded to conventions, it still did not issue any competent legislations to protect Palestinians’ data. A reality that warns of more violations and continued impunity under the

[21] “Access Now”, “viable to detection and exploitation: Protection of data in the MENA region”, January 2022. https://cutt.us/P4qG6

prevailing absence of legislation and an independent commission to regulate and institutionalize accountability of companies and authorities for any breaches, violations and other illegal interventions in privacy and personal data.