impact International accessnow

Privacy Violated:

Protection of Customers' Personal Information by Internet Service Providers in Palestine

August 2021

This study is a publication of Access Now and ImpACT International for Human Rights Policies. It is written by Nesma Jabr, Marwa Fatafta, and Dima Samaro. We would like to thank those who provided support, including Kassem Mnejja and Donna Wentworth.

Access Now defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, legal interventions and convenings such as Rightscon, we fight for human rights in the digital age.

www.accessnow.org

ImpACT International is concerned with policies at the intersection of states and businesses. It monitors and delivers technical advice on human rights to governments, international bodies, national institutions and influential corporations.

www.impactpolicies.org

24 August 2021

For more information, contact:

Marwa Fatafta

marwa@accessnow.org

Sarah Burashed

info@impactpolicies.org

Contents

I. Introduction

Internet use in the Occupied Palestinian Territories of East Jerusalem, the West Bank and Gaza (hereinafter "Palestine") has grown exponentially in the last decade. Between 2010 and 2019, the number of people using High Speed ADSL Internet has increased by 205%, now reaching a total of 363,000 users. [1]

Along with this dramatic growth has come threats to users' privacy, particularly related to the collection, use, and processing of their personal information. Internet Service Providers (ISPs) customarily collect users' personal data, use and share it in various ways and

1 https://bit.ly/3syKjmq

for multiple purposes. In the absence of appropriate regulations in Palestine, there is a growing concern regarding potential abuse and misuse of customers' personal information collected by ISPs, including regarding the purposes for which this data is used, and who it is shared with. Unfortunately, as this study demonstrates, customers in Palestine are not aware of their rights or the fate of their personal information.

To investigate the extent to which ISPs in Palestine respect the privacy of their customers and protect their personal data, ImpACT International for Human Rights Policies and Access Now review in this study the privacy policies published by seven major ISPs operating in Palestine. Our analysis reveals the privacy violations committed by ISPs as well as the lack of customers' awareness, both in terms of their rights and how their personal information is used.

II. Study Methodology

The study reviewed seven major ISPs that operate in Palestine which have a public privacy policy: Hadara, Mada, Fusion, Call U, Super Link, B Net and Zaytona. The study first examined the privacy policies published on the companies' official websites to determine the extent to which the firms respect and protect personal data. In the second phase, randomly selected customers were surveyed to assess their awareness of the policies and their individual rights related to the collection, use and sharing of their personal data.

III. Study Findings

A. Companies' privacy policies

Criteria for effective privacy policies

IMPACT International and Access Now initially reviewed the websites of twelve ISPs in Palestine. We found that only seven publish a privacy policy on their websites, which means that the customers of the other five companies have no information about the extent to which their data is protected.

The study team contacted the administrations of the five companies which do not have a public privacy policy to inquire about the issue. One company responded by publishing a policy on its website. The other four companies did not respond or act. Thus, we reviewed the privacy policies of the seven companies that published them, assessing whether they:

1. Are easy to find on the company's website;
2. Explicitly list the types of personal information collected from customers;

3. Describe how customers' personal information is collected;
4. List the purposes for which personal information is collected;
5. State that customers' have the right to object to the sharing of their personal data with third parties;
6. Explain the extent to which the ISP is legally responsible for protecting customers' personal information;
7. Disclose any third parties that are given access to customers' personal information, the purpose and the extent of their liability in the case of misuse;
8. Disclose customers' right to compensation if their personal information is stolen, leaked or used for other purposes;
9. Notify users if cookies are used on the website and if so, their type and purpose;
10. Explain any special attention given to protecting children's privacy;
11. Notify customers when the privacy policy is changed;
12. Explain how customers can contact the company with questions or concerns; and
13. State the legal authority to which customers can turn if they want to file a complaint.

Availability

Websites are typically the primary way ISPs inform users of their services and policies. We found that four of the seven ISPs we examined publish their privacy policies on their websites in an easily accessible way. Others, however—such as Hadara (affiliated with the Palestine Telecommunications Company, otherwise known as the Paltel Group) and Call-U—bury their policies, requiring customers to navigate from one page to another in order to find them.

In addition, both Fusion and Call-U publish their privacy policies in English, even though their websites and services target Arabic-speaking customers. That makes reading and understanding the privacy policies nearly impossible for a very large percentage of users.

Is it easy to find the privacy policy on the company's website?

Hadara

No.

It cannot be found on the home page. Rather, users must click on "My Page" in the menu and then "Terms of Use" to access "Our Privacy Policy," where it is listed second.

Mada

Yes.

The privacy policy is shared in a separate section titled «Privacy Terms» linked from the home page of the company's website.

Fusion

No.

Although the privacy policy is published in a specific section on the website home page, it is written in English, which makes it almost impossible to read or understand by a very large percentage of Arabic-speaking users.

Call-U

No.

because it is not clearly accessible on the home page of the company's website. Instead, visitors must choose «Dalal» from the menu, which leads them to the privacy policy. Moreover, the policy is written in English, which makes it difficult for the majority of Arabic-speaking customers to understand.

Super Link

Yes.

The privacy policy can be found on the home page of the company's website, titled «Privacy Terms.»

B Net

Yes.

It is linked from the website's home page under the heading «Privacy Policy.»

Zaytona

Yes.

t is included on the website's home page under the heading «Privacy Policy.»

Types of the information collected

Six out of the seven ISPs assessed (Hadara, Mada, Call-U, Super Link, B Net and Zaytona) only partially explain the information they collect from their customers. They do not specify what types of data they collect but refer to a few examples in their policies, using phrases such as «for example,» «etc.» and «other information.» Such vague phrasing would allow companies to collect additional information about their clients without prior permission or notification regarding the nature of the data collected, used and retained.

One company, Fusion, is particularly vague, which gives it total freedom to collect and retain information in a way that violates the privacy of users.

Does the policy include an explicit list of the types of personal information collected from customers?

Hadara

No.

It does not clearly define the nature of information it collects from clients. It is also vague about when it collects personal data, saying, for example, «the personal information that we may collect.» The company only cites examples such as name, mailing address, date of birth, gender, phone number, fax number and email. The door is left open to collecting additional information:

«The personal information that we may collect may include, for example, your name, mail address, date of birth, gender, phone and fax numbers, your email address, etc.»

The company goes on to say it may collect personal information about customers' use of its services and internet search habits.

Mada

Yes,

but only partially. It cites examples of the information it may collect (name, email, birth date, gender, phone number, fax number and address) but leaves the door open to gathering other data by using words such as «for example» and «etc.»

The company does, however, identify the information it does not collect, such as customers' bank information. It warns users not to provide that information to any party acting in its name and says it is not responsible for the consequences if they do.

Fusion

No.

It only states that it may collect information such as phone numbers. Thus, the company is free to collect other data without being bound by any conditions.

Call-U

Yes,

but only partially. The company provides only examples of the types of information it collects, such as name, email, gender, IP address, browser information and demographics. It also states it collects and retains information users submit via the company's smart phone applications, such as their Facebook account.

Like most ISPs, Call-U uses the phrase «for example» before mentioning the information collected and ends with the phrase, «and so on.» By using such phrases, the statement remains vague and incomplete, leaving the door open to collect other information.

Super Link

Yes,

but not with any detail, and it keeps its options open with the phrase, «and other similar information.» Among the examples cited are name, email address, phone number and the documents collected to prove customers' identity.

B Net

Yes,

but incompletely. The company explains the nature of the information collected from users (name, mail address, date of birth, gender, telephone and fax numbers and email), then adds «and others»—a loophole that allows it to retain other data without customers' knowledge. The company does say it does not collect any financial information and advises customers to reject any such requests.

Zaytona

Yes,

but incompletely. It only cites examples of the information that it may collect from customers: name, place of residence, email, and phone and fax number. Using expressions such as «for example» and «others,» it leaves its options open.

Methods of collecting customer information

Some of the target companies cite the methods used to obtain customers' personal information, but few offer details.

For example, two companies; Call U and SuperLink, do not give any details about how they collect data from customers. Using the phrase «and so on,» two other companies, Hadara and Fusion, leave the door open to using any other ways of obtaining information.

Does the company explain how it collects customers' personal information?

Hadara

Yes, although it is not sufficiently specific.

Hadara states that it collects personal information from individuals when they become its clients, visit or log into Hadara electronic gateways, use any of its services, make purchases from one of its stores or distributors, use offers, participate in contests and communicate with the company. However, the company adds «etc.» at the end of its list of collection methods, which allows it to collect information in ways and situations it does not mention.

Mada

Yes.

It explains that it collects customers' information when they submit a subscription request for any service or product, purchase one of its products, subscribe to commercial offers and communicate with its staff.

Fusion

Yes,

although it keeps its options open by adding «etc.» at the end of its list. Fusion explains that it collects and retains information provided by customers when they create an account, post content and complete forms via the company's mobile application. It warns in another clause titled «collecting non-personal information» that when customers open its mobile application, company servers automatically record their IP address; location; device name, version, and the operating system; language used; the information searched for and the time and date. And then it adds «etc.»

Call-U

Not completely.

The company states that it automatically collects and stores customers' data during every interaction with its application, but does not give details.

Super Link

No.

It only states that it does not collect any information that customers do not voluntarily provide.

B Net

Yes.

It states that it collects customers' personal information when they submit a subscription request, purchase any product from the company or its distributors, participate in its contests and communicate with its employees.

Zaytona

Yes.

It collects personal information from customers when they submit a subscription request, purchase products from the company or its authorized distributors, respond to offers and communicate with its staff.

The purposes for which companies use customers' personal information

Super Link is vague. Hadara, Mada, B Net and Zaytona cite the purposes in specific clauses. Fusion simply states that it uses customers' «non-personal» information to identify potential abuse and to develop its statistical database.

Does the policy state the purposes for which the company collects customers' personal information?

Hadara Mada B Net Zaytona

Yes.

They all state that they use customers' personal information to evaluate and develop new services and products, complete agreed-upon transactions, collect payments, verify customers' identity when they contact the company, inform them of service changes and/or conduct complete research.

Fusion

Yes.

The company says it uses customers' information internally to analyze, develop and further improve its services and products.

Call-U

Yes.

The company declares that it uses personal information to improve customer service and answer customers' inquiries. It also has said it uses «non-personal» information to identify potential abuse and collect statistics on the use of its mobile application.

Super Link

Yes.

The company says that it uses the information only to carry out its operations, communicate with customers and respond to their requests.

Customers' right to data protection

It is important that ISP privacy policies inform customers of their right to protection of their personal data, including the ability to access or transfer their data upon request, to correct or even delete it, and to restrict its use in specific cases.

However, six out of the seven target ISPs (Mada, Call-U, Hadara, B Net, Zaytona and Super Link) do not explicitly state and explain these rights. Mada does not mention any information about customers' rights to privacy. Call-U mentions which information customers have the right to access or update. Hadara, Super Link, B Net and Zaytona simply state that customers may change their information if they desire.

Fusion stands out as the lone company in compliance with this requirement. Its policy includes a specific clause titled «Users' Rights,» in which it explains customers' right to withdraw their consent to use their information, to learn whether and how it was used by the company and to verify, modify, or update it. The policy also contains a clause titled «How to enjoy these rights.»

Legal responsibility for protecting customers' personal information

None of the ISPs acknowledge any legal responsibility for protecting customers' information, including their confidentiality. Even Fusion fails to include any details about its legal responsibility.

Moreover, Super Link explicitly strips customers of their right to take any legal action via the following clause: "... and the confidentiality of the information provided under this system is the responsibility of subscribers alone and they are not entitled in any way to file a complaint and/or lawsuit against Super Link.»

Is there a clear statement regarding the extent to which the ISP is legally responsible for protecting customers' personal information?

Hadara	Mada	B Net	Fusion
No	No	No	No

Call-U	Super Link	Zaytona
No	No It even deprives customers of their right to file any legal proceedings.	No

Sharing of data with third parties

Many ISPs do not disclose that customers' personal information may be accessed by third parties. For example, two out of the seven ISPs (Zaytona and Fusion) do not mention anything in this regard. Super Link states only that it «may» share customers' information with the national judicial authorities if necessary.

Hadara, Mada, B Net and Call-U reserve the right to share information, without committing to protecting customers' privacy.

Most of these companies do not explain the legal liability of the third parties in the case of misuse or harm.

Is clear notice given of any other parties that have access to customers' personal information, for what purpose, and to what extent are they liable in the case of any misuse?

Hadara Mada B Net

Hadara declares that it shares customers' information with «trusted» third parties in several cases. Both Mada and B Net follow the same policy.

When solution providers, business partners "and others" are needed to operate its websites and services, Hadara offers the reassurance that it discloses customers' information only 1.) If the third parties agree to limit use to permitted uses; 2) If the company is restructured or sold to a third party; and 3) If the company is required by law or «in good faith» to comply with a judicial order, or to defend or protect its rights or those of its customers or the citizenry in general.

However, Hadara does not address the legal liability of third parties if they use customers' information in a way that violates privacy or causes harm. Instead, it makes it clear that its privacy policy does not apply to third-party websites.

Mada and B Net share the same policy.

Fusion

It does not mention any details related to sharing information with third parties.

Call-U

It states that it shares customers' personal information with partners engaged in its Dalal application (in which case, the partners' privacy policy governs) and any other agents with which it cooperates. In the latter case, Call-U states that the agents only may use necessary customer information.

Call-U considers customer information an asset that can be sold or transferred to a third party if it goes bankrupt or is sold. In addition, like the other companies, Call-U states that it may share such data with judicial authorities if necessary to comply with the law or to protect the rights, property, or safety of the company, its employees, customers, "and others."

The company pledges that it will inform customers (and allow them to refuse) if it shares their information with any third party not otherwise mentioned.

Super Link

It states that it does not sell or rent user data to any third party, but it may be forced to share it with law enforcement or regulatory agencies.

Zaytona

It does not mention any details related to sharing information with third parties.

Customers' access to remedy in case their personal information is misused

None of the ISPs' privacy policies explain the customers' right to compensation if their personal information is stolen, leaked, published or used for purposes not covered in the privacy policy, or if their rights are violated in any other way.

Hadara, for example, relieves itself of responsibility for loss of customer information, damage or harm. In a paragraph titled «Denial of Liability and its Limits,» it states that it offers no guarantee, explicitly or otherwise, regarding its service or content. The company reminds customers that it provides its service on an «as it is» and «as available» basis, and that if they do not like the terms and conditions of the subscription, they should terminate the relationship.

Does the company guarantee customers' rights to compensation if their personal information is misused?

Hadara	Mada	B Net	Fusion
No	No	No	No

Call-U	Super Link	Zaytona
No	No	No

Use of cookies

Cookies (called web cookies, internet cookies and browser cookies) are small pieces of data stored on users' computers by the browser while they surf a website. Cookies allow websites to "remember" users and their preferences, which helps assure that the experience caters to their needs, including customized advertising and the ability to instantly log on.

Privacy policies are expected to inform visitors of the use of cookies. However, only Hadara's privacy policy does so. Hadara states in a special clause that it uses cookies to provide better customer service. It lists five purposes of cookies: identify and respond to users' personal preferences, show users appropriate advertisements, collect statistics, learn how users find the company's website and make emailed offers more relevant to customers. The company reassures readers that it does not use cookies to analyze users' visits to other websites.

Does the company inform its website visitors of the use of cookies?

Hadara	Mada	B Net	Fusion
Yes	No	No	No

Call-U	Super Link	Zaytona
No	No	No

Children's privacy

The privacy policies of Fusion and Call-U include a special clause on children. They state that they do not collect any personal information from children under the age of 13. None of the other ISPs address this issue in their published privacy policies.

Does the company mention how it handles children's personal information?

Fusion Call-U	Mada	B Net	Hadara
Yes. They state that they do not collect any personal information from children under the age of 13.	No	No	No

Super Link	Zaytona
No	No

Notification of modifications

All of the target ISPs in Palestine reserve the right to change the terms and conditions of their privacy policies when they deem necessary. However, five of the ISPs (Hadara, Mada, Super Link, B Net and Zaytona) do not pledge to notify customers if they change or amend their privacy policies. Only two (Fusion and Call-U) say they do.

Are customers notified when the privacy policy is changed? Is it stated how that notification occurs?

Hadara

No.

Hadara reserves the right to amend its privacy policy at any time but does not mention whether it informs customers.

Mada

No.

Mada reserves the right to amend its privacy policy when required, saying only that changes will be published on its website. Customers are not notified when the privacy policy is changed.

Fusion

Yes.

Fusion states that it may amend the policies related to its mobile app or services at any time. It promises to notify customers of the change via its mobile application; when customers log on, they are prompted to accept the changes.

Call-U

Yes.

Call-U can change its privacy policy at any time, and it informs customers by email or when they log on to the website.

Super Link

No.

Super Link reserves the right to rewrite its privacy policy when necessary. It does not mention whether and how it informs customers of the changes. Rather, it only says that the new policy becomes binding on subscribers once it is implemented.

B Net

No.

It can change the terms and conditions of its privacy policy when it deems appropriate, and these changes are published on the relevant page of the website. B Net does not state how it informs its customers of these changes.

Zaytona

No.

It does not mention anything in this regard.

Methods for contacting the company

All of the ISPs except for Super Link ask customers to contact the company with any comments or inquiries. However, Hadara and Fusion do not explain how.

Legal remedies

None of the companies explicitly mention anything related to the legal authority to which customers can turn if they do not adhere to the terms stipulated in their privacy policies.

> Call-U, for example, states that all damages or disputes are subject to California law—a clear indication that it had merely (and sloppily) copied the privacy policy of another company without reviewing or checking it.

On the other hand, Super Link states that its policy is subject to the prevailing laws in Palestine.

Summary

After analyzing and comparing the privacy policies of the seven ISPs (Hadara, Mada, Fusion, Call-U, Super Link, B Net and Zaytona), ImpACT International for Human Rights Policies and Access Now conclude that all of the companies fail to meet the standards for privacy and data protection.

Since the majority of the ISP privacy policies in Palestine do not include clear details on the rights of users, customers remain unaware of what ISPs can do with their personal data, including sensitive and confidential information.

Moreover, all ISPs relieve themselves of any legal liability for the misuse or loss of customers' information and do not inform them of their right to compensation.

The following table summarizes how the target ISPs deal with the various elements that should be included in a privacy policy:

	Elements of a privacy policy	Hadara	Mada	Fusion	Call-U	Super Link	B Net	Zaytona
.1	Easy access to privacy policy	No	Yes	No	No	Yes	Yes	Yes
.2	Nature of the information collected	Not all of them	Not all of them	No	Not all of them	Not all of them	Not all of them	Not all of them
.3	Ways of obtaining information	Yes, but it leaves the door open to collecting info in other ways	Yes	Yes, but it leaves the door open to collecting info in other ways	Not precise	No	Yes	Yes
.4	Purposes of collecting information	Yes	Yes	Yes	Yes	Yes	Yes	Yes
.5	Rights to protecting personal data	No	No	Yes	No	No	No	No
.6	Legal responsibility	No	No	No	No	No	No	No
.7	Sharing data with third parties	Yes	Yes	No	Yes	Not clear	Yes	No
.8	Right to compensation	No	No	No	No	No	No	No
.9	Cookies	Yes	No	No	No	No	No	No

.10	Children's privacy	No	No	Yes	Yes	No	No	No
.11	Notification of privacy policy changes	No	No	Yes	Yes	No	No	No
.12	Ways to contact the company	Yes, but without explaining how	Yes	Yes, but without explaining how	Yes	No	Yes	Yes
.13	Legal authority to which customers can turn	No	No	No	No, but it says its policies are subject to California law	No, but it says its behavior with customers is subject to Palestinian laws	No	No

V. Customer awareness of privacy rights

To assess the level of customer awareness of their right to privacy and the degree to which their personal information is protected by ISPs, ImpACT International and Access Now conducted personal interviews and an online quantitative survey. The questionnaire was directed to a random sample of residents of the Gaza Strip and the West Bank via email and on social media.

In addition to demographic questions (gender, age, place of residence, educational level and profession), two types of information were collected from ISP customers:

1. Awareness of privacy policies:

- Do they know what a privacy policy is?
- Do they read the privacy policy when subscribing to a service?
- Do they know the essential elements of an effective privacy policy?
- Have they ever researched the laws that exist to protect privacy in Palestine?
- Have they read Palestine's cybercrime legislation?

2. Extent of knowledge of how their own ISP collects, stores, uses and shares their personal data:

- When they are contacted by an ISP employee about a subscription, are they questioned about their identity?
- What personal information is requested and verified?
- Are they asked for sensitive information such as bank account number or credit card specifics?
- Are customers concerned about the risk of their private information being revealed or shared without permission?
- Has an ISP ever requested permission to use or share their personal data with third parties?
- Do they wish to be notified or asked for permission before their information is used or shared?
- Do they think ISPs share their personal data with third parties (e.g. private companies, the public prosecutor, government entities, etc.)?
- Do they know their rights when it comes to the privacy of their personal information?
- Do they believe a law should be enacted to protect citizens' personal data?

- Are they aware of their right to compensation if ISPs disclose, exploit, or steal their personal information?
- If their information is stolen, disclosed, or exploited without prior permission, do they know how to demand their rights?
- Do they trust ISPs to maintain the confidentiality of their personal information?

Below is a summary of what we learned:

Demographic characteristics:

The field research team conducted 54 interviews with customers of the target internet ISPs. Of those, 49.3% were residents of the West Bank and 50.7% live in the Gaza Strip. Of the 209 customers who answered the questionnaire, 46.9% were residents of the West Bank and 53.1% of the Gaza Strip.

Of those who completed the online questionnaire:

- 66.5% were women.
- 52.4% were 2540- years old. Of the remainder, 28.2% were 16 to 25 years old and 19.4% were 40 to 60.
- 65.7% held a bachelor's degree and 46.7% were employed by a company or organization. Another 25.7% were students and the rest were either self-employed, unemployed homemakers or retired.

Customer attitudes toward privacy policies

About a third of the respondents in both the interviews and survey (30.8%) said they do not know what «privacy policy» actually means. When subscribing to any service,

more than 33% of the respondents do not read the privacy policy before approving it, while 36.2% only read it occasionally. Likewise, 36.4% of the respondents said they do not know the elements that should be included in a privacy policy, while 48.5% said they know only some of them.

Most of the respondents (68.9%) have never researched whether a particular law exists to protect customer privacy in Palestine. In addition, 73.8% say they have never read the Palestinian Cybercrime Law, while 13% said they had no clue that it even exists.

Nature of personal information collected

Almost half of the respondents reported that ISPs always inquire about their identity when contacting them. Most participants also said that in addition to their name, their phone and ID are the most frequently requested information (see Figure 1). However, most of the respondents (more than 94%) reported that they have never been asked for sensitive information such as their bank account.

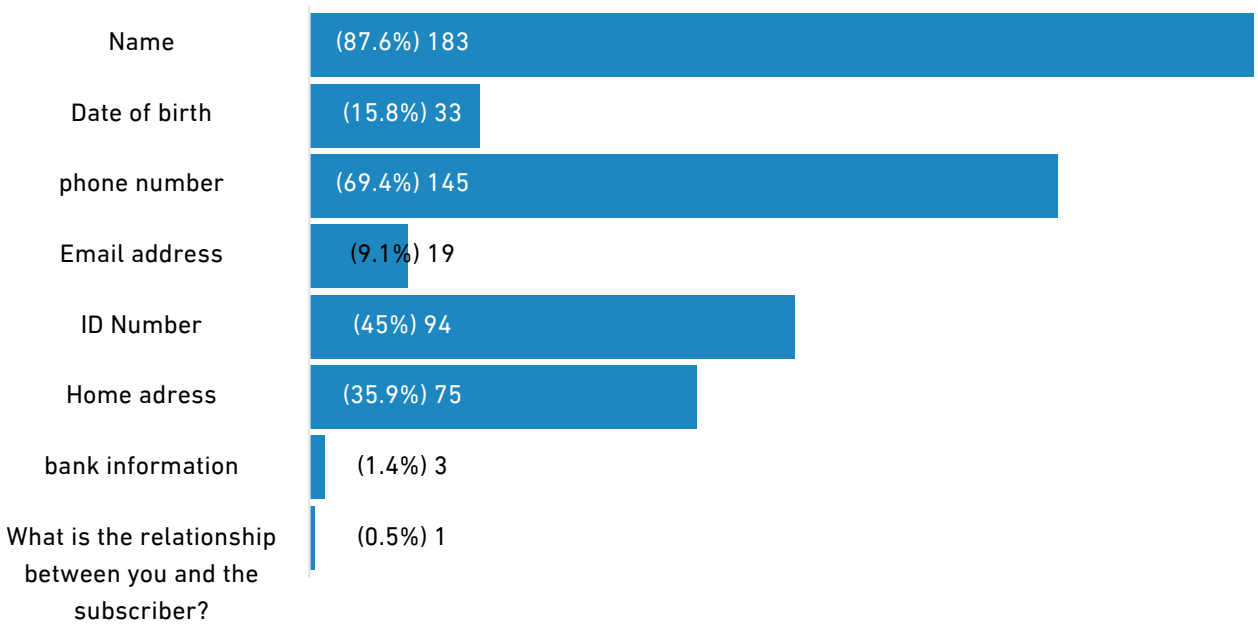


Figure 1: The nature of information requested when ISPs contact customers

Sharing information without customers' permission

More than 90% of the respondents believe prior permission should be required before private information is disclosed or shared. Approximately 67% said they have not been asked by an ISP for such permission, while about 26% do not remember if they have received such an inquiry.

However, approximately 95% of participants confirmed that they want to be notified and asked for permission if an ISP plans to share their information with a third party.

Awareness of the existence of a third party

About a third of the people we questioned assumed that internet service providers share their information with third parties (see Figure 2), but most (87.6%) say they've never been informed or asked permission for such sharing.

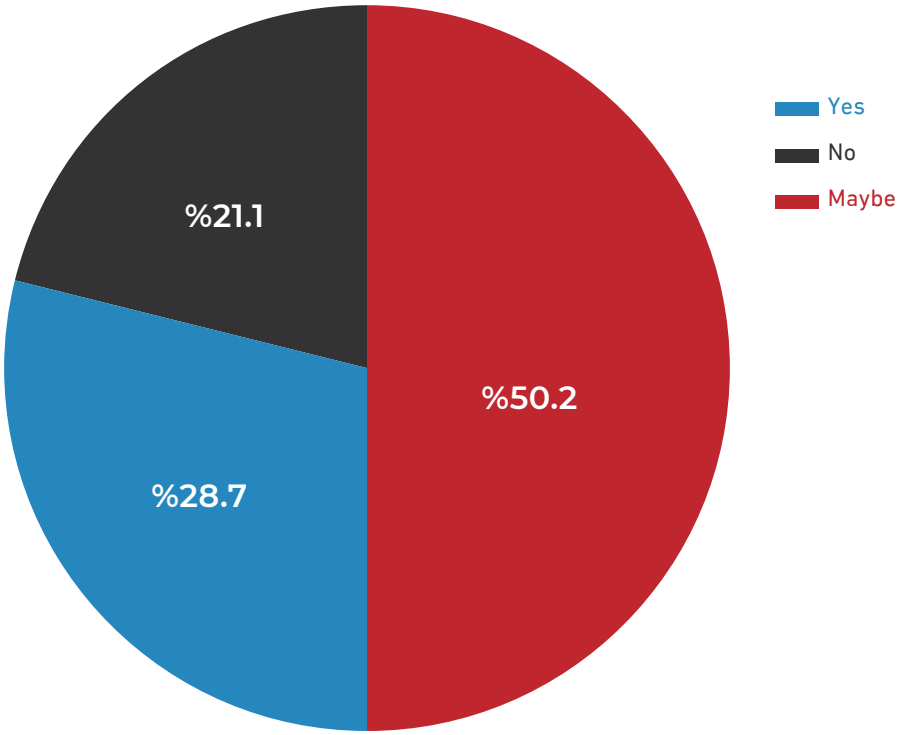


Figure 2: Awareness of the existence of a third party

Awareness of privacy rights

Most of the respondents were not aware of their right to privacy and consent when it comes to ISP use and sharing of their personal information (Figure 3).

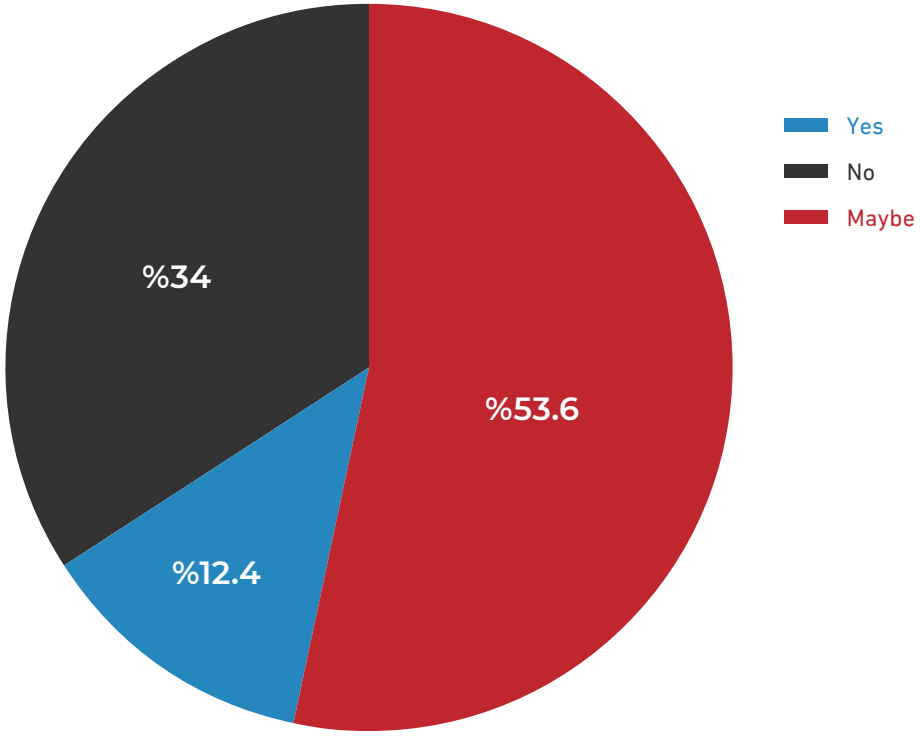


Figure 3: Awareness of the right to personal data protection

Right to compensation:

When asked if they believe they have a right to compensation if an ISP discloses or exploits their personal information, 76.4% said yes, while 9.1% said no. The other 14.5% were not sure.

Remedies in the case of misuse or fraud

Almost half of the customers queried (48.3%) said they didn't know what remedies would be open to them if their personal information was disclosed or exploited; 18.2% claimed to be aware (see Figure 4).

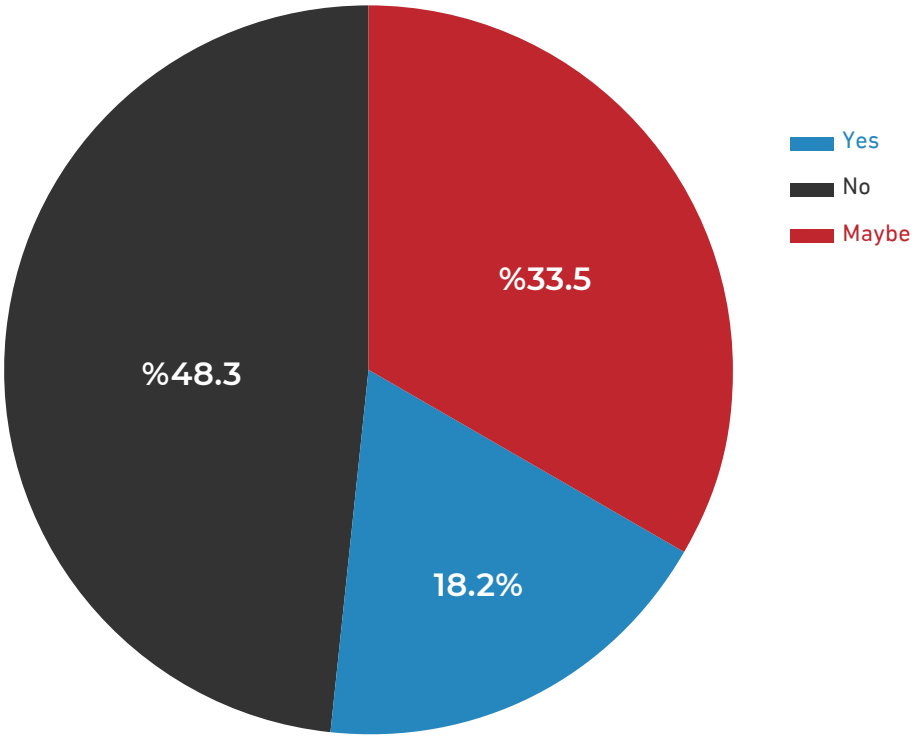
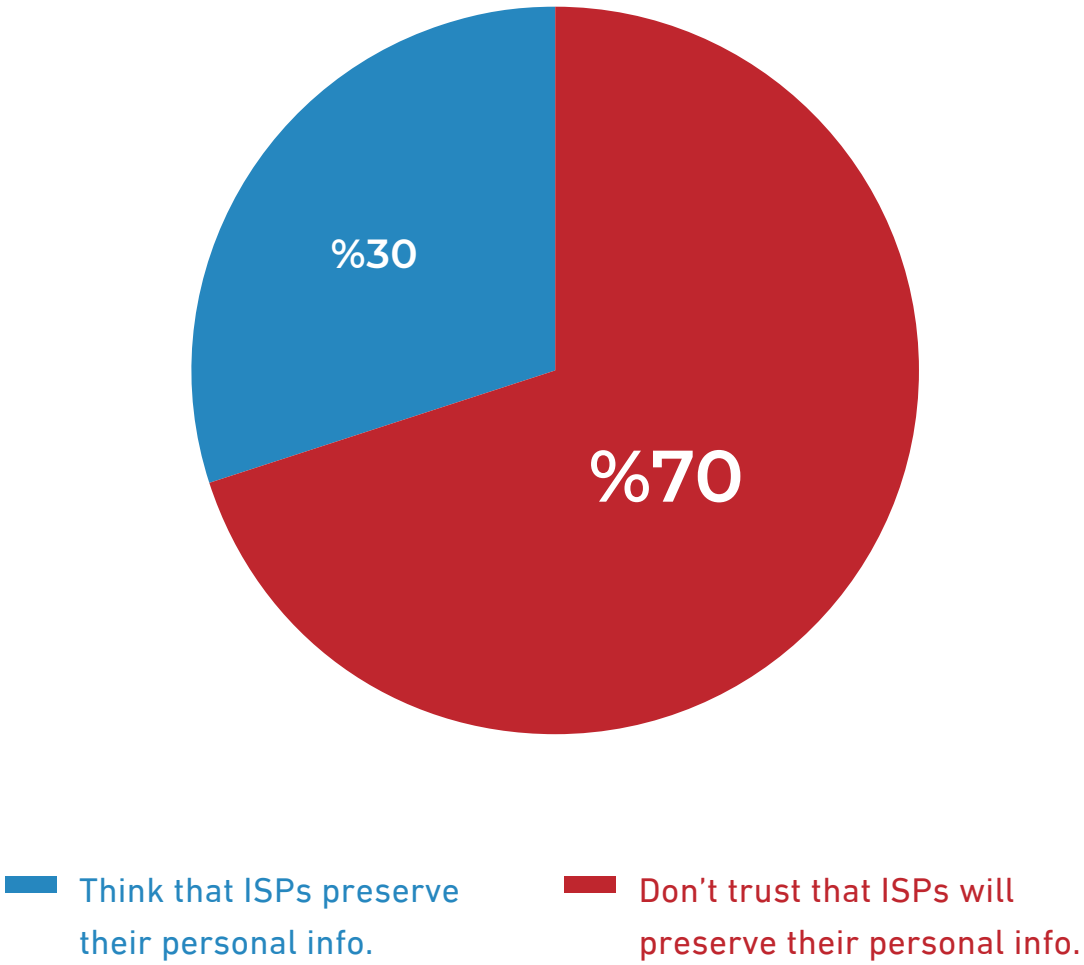


Figure (4): What can be done in case of fraud

Trust in internet service providers:

Nearly 70% of respondents do not trust that internet service providers will preserve the confidentiality of their personal information, and 94.7% say it's critical for governments to enact a law to protect citizens' personal data.



Summary of customer responses:

About one third of respondents (30.8%) are unaware of how a privacy policy can and should protect them, while another third (33%) know about it but do not read it when subscribing to a service. In addition, most respondents are not fully aware of how ISPs use their personal information or with whom they share it, and don't know how to seek redress if abuse occurs. This lack of awareness and action works to the advantage of ISPs, paving the way to push customers to sign subscription contracts without informing them of their rights or asking them to approve it before committing. At the same time, however, about two-thirds of respondents do not trust ISPs' commitment to confidentiality and would support enactment of a law to assure their privacy is protected.

VI. Legal Framework:

absence of adequate safeguards for personal data

The Palestinian Basic Law, which serves as the constitutional framework for the Palestinian legal system, criminalizes "any violation of any personal freedom, of the sanctity of the private life of human beings, or of any of the rights or liberties." [1] It also guarantees Palestinian citizens access to fair remedy if their fundemental rights have been violated. In practice, however, there have been only limited efforts by the Palestinian Authority (PA) to protect the privacy of Palestinian individuals and safeguard their personal information. [2]

The Cybercrime Law (No. 10 of 2018) prohibits unlawful access to information systems, sharing intercepted records or data and arbitrary or interference with privacy with imprisonment and heavy fines. Notably, Article 4 prohibits unlawful access to information systems which could result in "deletion, addition, disclosure, destruction, alteration, transfer, capture, copy, dissemination, reproduction or attachment of data or electronic information." Article 7 also penalizes anyone who intentionally and unlawfully receives, records or intercepts any data by at least one year in prison and a fine between 1,000 and 3,000 Jordanian Dinar. Additionally, Article 22 prohibits "arbitrary or illegal interference with the privacy of any person or the affairs of his family, home or correspondence," and the dissemination of the information thereof. On the other hand, Article 32 of the law obligates ISPs to retain users' data for at least three years and grants the public prosecutor the right to collect unrestricted

1 Article 32 of the Amended Basic Law of 2003. Retrieved July 2021 ,30, from https://www.elections.ps/Portals/0/pdf/The_Amended_Basic_Law_2003_EN.pdf

2 For more information on data protection in Palestine, read Access Now's paper "Exposed and Exploited: Data Protection in the Middle East and North Africa," January 2021 https://www.accessnow.org/cms/assets/uploads/01/2021/Access-Now-MENA-data-protection-report.pdf

data such as private communications, traffic data, and metadata. It's worth noting that Israel, as an occupying power, does not apply its Protection of Privacy Law (PPL) of 1981 and guidelines of its Privacy Authority (established in 2006) to Palestinians in the West Bank and the Gaza Strip.

To date, there is no data protection law in Palestine, nor an adequate legal framework, to safeguard the right of internet users to privacy or require telecom companies and ISPs to provide access to grievance mechanisms to those adversely affected by their policies and operations related to processing of personal data.

V. Recommendations:

To companies:

1. Adopt and enforce a robust, right-respecting and user-centric privacy policy to protect users' personal data

As demonstrated in the report, none of the seven ISPs are committed to respecting customers' right to privacy and ensuring the protection of their personal dara, opening the door to abuse and privacy violations. Therefore, all ISPs in Palestine should be mandated to amend their privacy policies to ensure customers' rights are protected. A robust privacy policy should include the following elements:

- Specific types or categories of data collected from customers and how it is used, without loopholes.
- A clear, easy-to-understand statement of customers' rights, including the right to consent, to access personal information, to modify or delete data, to restrict its use and to object to how the company uses it.
- An explanation of cookies the ISP uses and their purpose, as well as how customers can refuse them.
- The legal responsibility of the ISP and any third party with which it shares personal data.
- Customers' right to compensation in the case of data leakage or misuse.
- The legal authority to which customers can turn to file a complaint.
- How to contact the company.

2. Ensure your privacy policy is public and easily accessible to users

ISPs should publish their privacy policies on their websites where they can be easily accessed, and they should be made available in both Arabic and English in order to be accessible and comprehensible to all of their customers.

Furthermore, ISPs should notify and inform their users whenever their privacy policies are updated or modified.

In addition, those Palestinian ISPs that collect personal information from customers who are EU citizens must comply with the rules of the General Data Protection Regulation (GDPR).

3. Collect only the data necessary to provide products or services

Following the principle of data minimization, ISPs should collect the only data necessary for the purpose of providing their products and services. ISPs should limit the scope of data collected out of the immediate and necessary purpose for which data is collected as well as limit the period of data retention in order to avoid potential harms caused by leakages, negligence or surveillance.

To the Palestinian Authority (PA):

1. Impose government regulations

The lack of regulation of the internet service providers and the absence of a specific law governing the privacy of personal information has contributed to the failure of these companies to make it a priority. Therefore, it is necessary to amend the laws and policies in force in Palestine to mandate the privacy of customers' personal information. In addition, the Ministry of Communications and Information Technology in Palestine should monitor ISPs to ensure their commitment to protecting users' information.

2. Enact a robust data protection law

The PA must prioritize the adoption of a robust data protection law that centers the fundamental rights of users over the financial interest of private companies. To that end, Access Now developed a guide for lawmakers, Creating a Data Protection Framework: A Do's and Don'ts Guide for Lawmakers, building on our experience and lessons from the EU's General Data Protection Regulation (GDPR). [1]

A framework aiming to protect personal data and guarantee users' agency and control over their personal information must include binding rights for users, including their right to explicit consent, object, erase, rectify and access their data.

3. Raise awareness of the right to privacy of information

A large number of customers do not know they have a right to protection of their personal information, cannot gauge the extent to which internet service providers respect the confidentiality of their data and do not understand how to demand redress if it's misused.

Accordingly, ImpACT International for Human Rights Policies and Access Now call on the Palestinian Ministry of Telecommunications and Information Technology to work withcivil society organizations to launch an awareness-raising campaign to educate residents on the importance of becoming familiar with the privacy policies of their ISP and demanding their right to the privacy.

1 https://www.accessnow.org/cms/assets/uploads/11/2019/Data-Protection-Guide-for-Lawmakers-Access-Now.pdf

Special thanks to:

Marwa Fatafta

MENA Policy Manager – Access Now

Kassem Mnejja

MENA Campaigner – Access Now

Dima Samaro

Consultant, Tech Policy Expert

Khalil Agha

Digital Media Advisor

Donna Wentwort

Editor

Rohdé te Paske

Editor

Paul Attenborough

Editor

Nesma Jaber

Researcher

Sari Noah

Researcher

Sarah Ali

Field researcher

Ahmed Mousa

Field Researcher

Laura Hayek

Translator

Mustafa Jihad

Designer