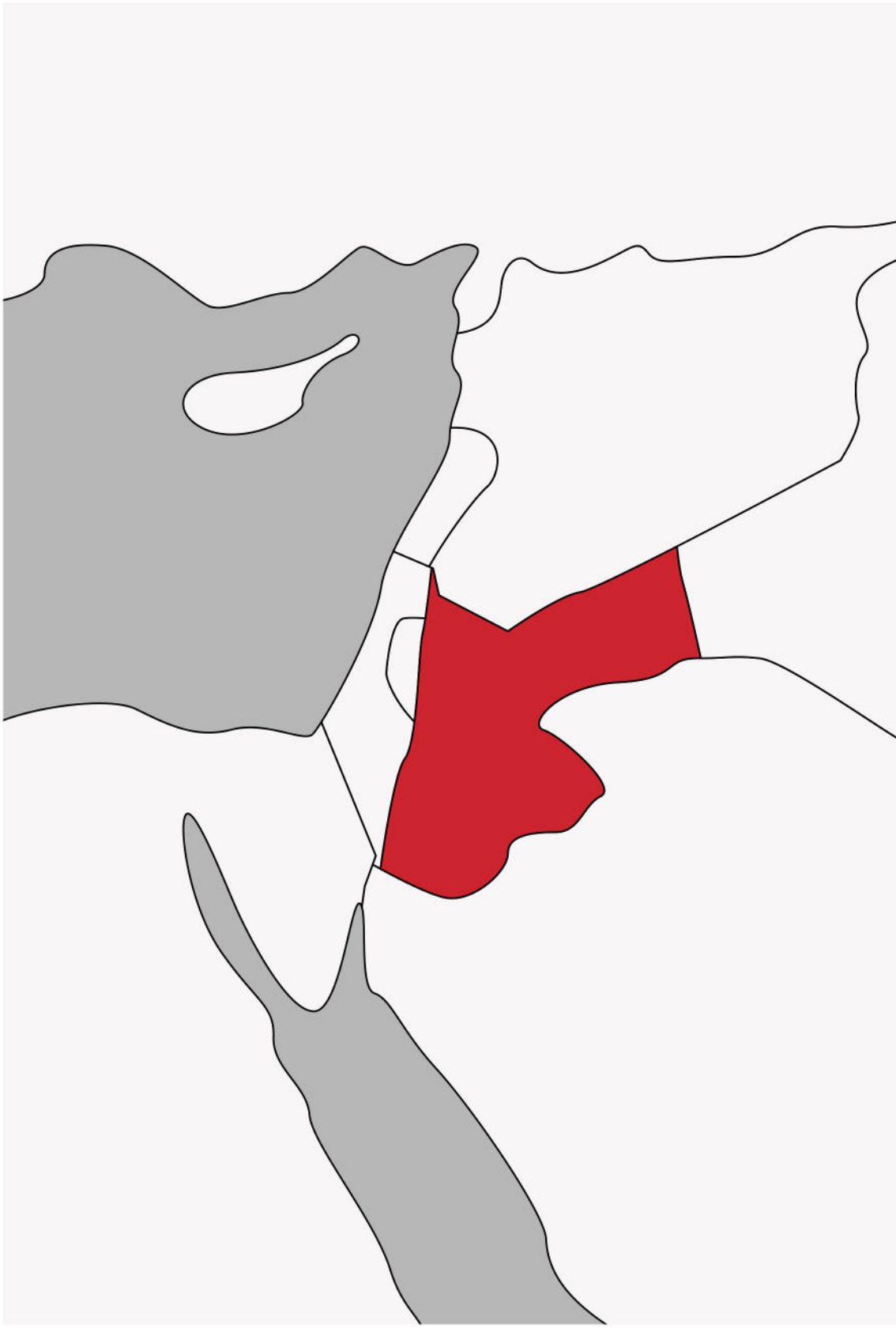
impACT International

accessnow

Violated Privacy:

Internet Companies' handling of customers' personal information



Contents

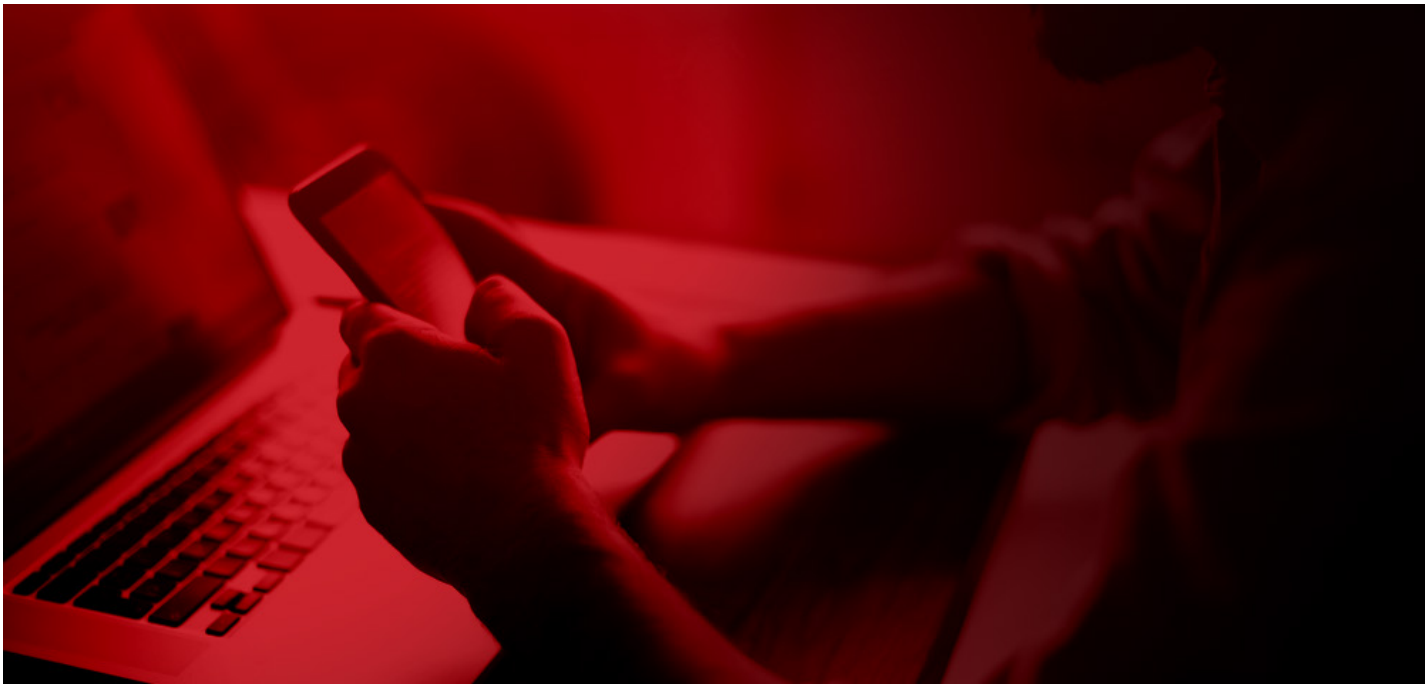
Introduction	4
Study methodology	6
Comparison of privacy policies	7
Awareness of privacy policies	17
Consumer knowledge about privacy protection	19
Recommendations	25

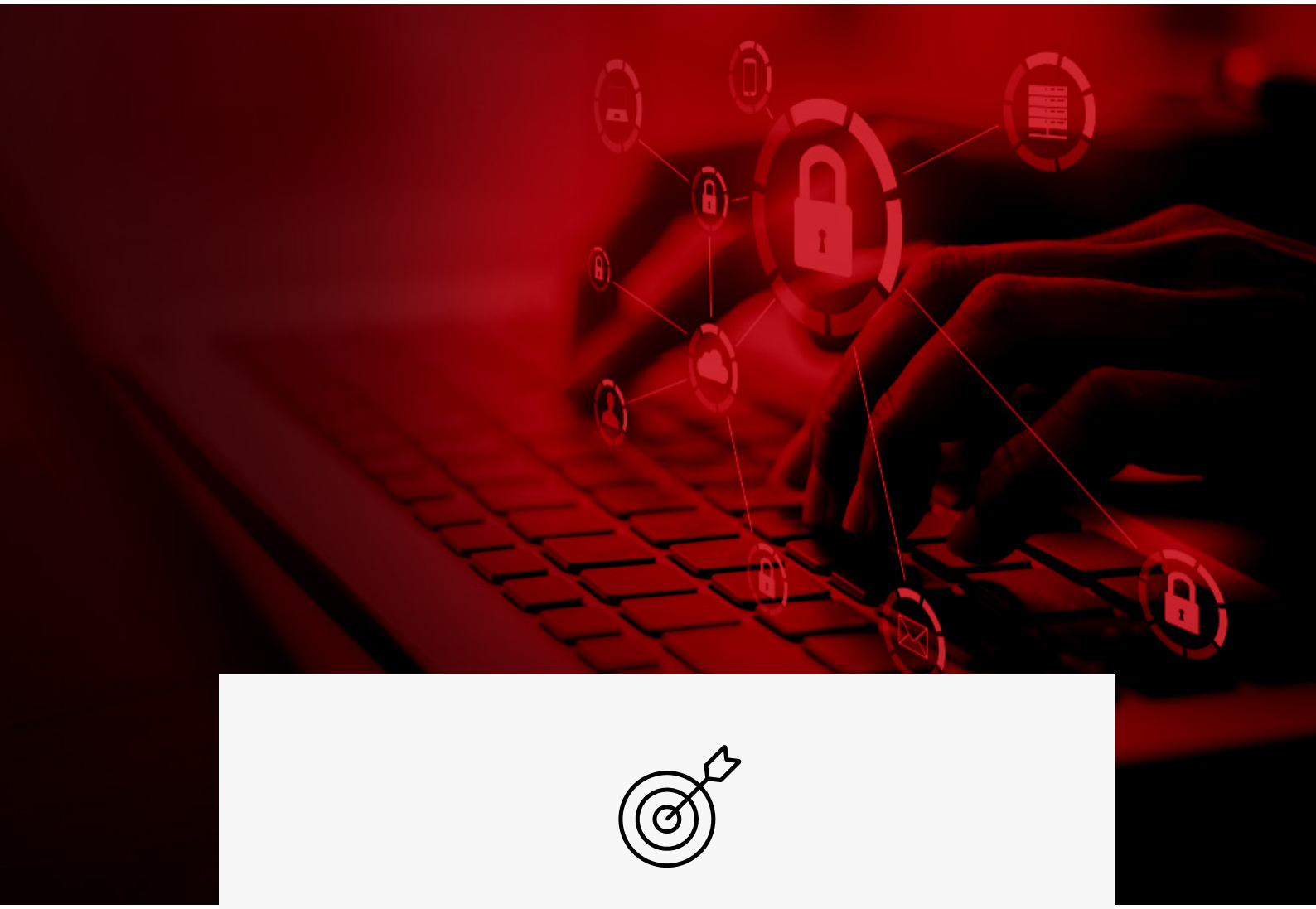
Introduction

With the growing importance of the internet to nearly every facet of modern life, the potential for abuse both by governments and private interests is increasingly real and significant. Telecommunication companies and internet service providers (ISPs) require customers to divulge a growing volume of personal information that, in the wrong hands, can be—and has been—used to destroy reputations, punish holders of dissenting points of view, bilk owners of savings, and limit access to internet in case of internet shutdowns. That facet has triggered concerns among the public and privacy experts about where this information is stored, for how long it is stored, who is entitled to access it, how it is applied and whether customers are aware of their rights.

Thus, ImpACT International for Human Rights Policies and Access Now

are conducting a series of analyses of ISP policies and practices in the Arab world, beginning with the Hashemite Kingdom of Jordan. The Telecommunications Regulatory Commission estimates that the country's internet subscriptions have reached 9.1 million, representing more than %90 of households.





The focus of this study is on five of the most prominent ISPs in the country (Zain, Orange, Umniah, TE Data and Damamax), hoping this will lead to improved privacy policies and practices across the local industry. The analysis also measures customer awareness of the use of their personal information, the legal authority responsible for protecting its privacy and their right to compensation, remedy, and appeal appeal in case of loss, breach or misuse of this information.

Study methodology

The five ISPs examined were Zain, Umniah, Orange, DAMAMAX and TE Data. First, ImpACT and Access Now reviewed and compared the privacy policies published on their websites. The second step was a questionnaire that assessed awareness by ISP staff of the importance of protecting users' personal data and the extent to which the companies share such information with third parties. The third step was a survey of customers' attitudes related to sharing personal information

Comparison of privacy policies

The privacy policies of the five major ISP companies were reviewed by the ImpACT and Access Now teams from six perspectives, as shown in the following table: types of information collected; how personal data are used, for what purposes and where; with whom personal data are shared, if anyone; customers' right to compensation if their information is stolen or disseminated/used in violation of the privacy policy; and a third party's degree of liability in case of the latter.

Is there is a clear, complete and official definition and disclosure of what personal information is collected from customers?

Zain

No;
the statement is vague and incomplete. "The type of personal information we may collect could include, for example, your name and postal address, date of birth, gender, telephone and fax numbers, email address and more." [Emphasis added]

Umniah

Yes;
but the statement is vague. "The company shall, without limitation, collect the following personal information and data: username and postal address, user's date of birth, user gender, telephone and fax phone numbers, user email, and other information collected on registration or through surveys." [Emphasis added.]

Orange

No.
The information collected from subscribers is not mentioned at all.

DAMAMAX

No.
The information collected from subscribers is not mentioned at all.

TE Data

No.
The information collected from subscribers is not mentioned at all.

Is there clear, complete disclosure of where personal information is used and for what purposes?

Zain

Yes.

Umniah

No,
it only states that the information provided by the user is fit for publication and it has the right to use it in future services.

Orange

No.

DAMAMAX

No.

TE Data

No.

Does the privacy policy explain customers' rights to compensation if their personal information is stolen, disseminated or used for purposes other than those disclosed?

Zain

No,

Umniah

No,

Orange

No.

DAMAMAX

No.

TE Data

No.

If personal information is shared with third parties, is it disclosed, along with the circumstances?

Zain

No.
The statement is vague and contains a loophole: "These companies can be content providers, business partners or otherwise [emphasis added]. We share with them to offer you different services and solutions".

Umniah

No.

Orange

No.

DAMAMAX

Yes

TE Data

Yes

Is there clear, complete disclosure of the situations in which personal information is shared with third parties?

Zain

No..

Umniah

No.

Orange

Yes.
The company may disclose your personal data, acting in good faith, if it believes that such action is necessary to: (i) conform with a legal requirement;
(ii) comply with a legal process; or
(iii) defend the rights or property of Orange

DAMAMAX

Yes.
The first party is committed to maintaining the confidentiality of the second party›s information and not disclosing it, except when the second party agrees to share it or the information to is demanded by security or judicial authorities via a formal request.

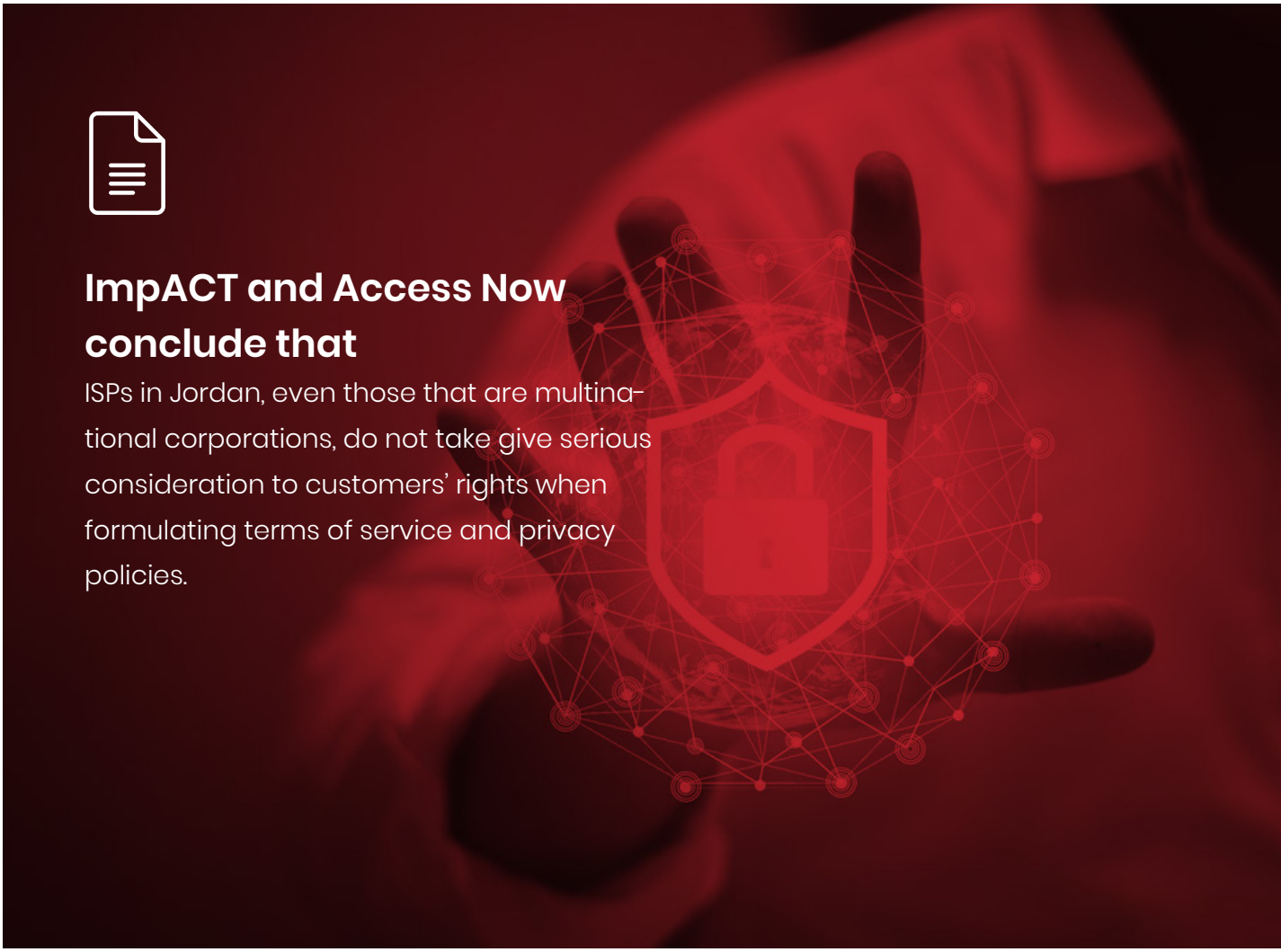
TE Data

Yes.
The first party is committed to maintaining the confidentiality of the second party›s information and not disclosing it, except when the second party agrees to share it or when it is formally requested by security and judicial authorities.

Is the legal liability explained for any third party responsible for a loss, breach or misuse of personal information?

Zain	Umniah
No.	No.

Orange	DAMAMAX	TE Data
No.	No.	No.



ImpACT and Access Now conclude that

ISPs in Jordan, even those that are multinational corporations, do not take give serious consideration to customers' rights when formulating terms of service and privacy policies.

Nature of customer information collected

ImpACT and Access Now found that some ISPs clearly violate their customers' privacy, while at the same time, the latter do not realize to what extent their personal data are being collected and used. Two of the five major players list the customer information collected and retained but include an "other" category that allows exceptions. One simply says it will collect any information it deems helpful in identifying other products or services to promote. And two say nothing at all on the issue.

When it comes to disclosing where and how personal information is used, only two of the companies were forthcoming, whereas three companies remained silent, and did not include or indicate any further clarifications. And only three list the circumstances in which they will share personal data.

For instance, Umniah explicitly states that it collects and retains personal information in a way that violates customers' privacy. In section 1.2.3 of its privacy policy,

> Umniah says, "The company may collect information about your visit and use of the site and/or services, including the pages you view, the links you click and other actions taken in connection to the site and/or services. The company shall also collect certain standard information that your browser sends to every website you visit."

Likewise, in its "Information Security Management and Privacy Policy,

> " Zain declares that, "The type of personal information we may collect could include, for example, your name and postal address, date of birth, gender, telephone and fax numbers, email address and more."

Although it may seem banal, the phrase "and more" leaves the door wide open for collection of virtually all types of personal data, and without individuals' explicit consent.
The privacy policy published by Orange does not explain the nature of customer information collected, how it is used, or the exact and clear purposes of the collected data, only stating that it "will not share your email with a third party."
The Damamax privacy policy also is vague. The company merely states in section 4-2 of its subscription contract that, "The first party commits to maintain the confidentiality of the second party's information and not disclose them except for the information approved to be disclosed by the second party or the information that is disclosed according to the request of the security and/or the judicial authorities and/or based on an official request." No description is offered of the nature of the information collected and retained. This gap in the Damamax privacy policy allows the company to collect personal information without seeking prior approval, or even informing customers. Thus, this will grant the company a huge capacity to misuse the personal data for unknown purposes.
TE Data follows suit. In its "Terms and Conditions of Internet Services," the company states that "we maintain the confidentiality of the second party's information and do not disclose them except for the information approved to be disclosed by the second party." No mention is made of the nature of the information collected and retained.
None of the five companies address customers' rights to compensation when information is stolen or otherwise illegally disseminated or used, none are public about recipients when data are shared, and none discuss legal liability. In most cases, there is no remedy at all, since there are no record of appeal and remedy cases on ground.

Purpose of use of personal customer information

In its "Information Security Management and Privacy Policy," Zain states vaguely that "we collect your personal information because we want to serve you customized offers and to enhance your user experience with us." It promises to treat all "personally identifiable information in strict confidentiality." It is not clear if this would mean targeting those who are using Zain with ads. The customers might be targeted specifically based on demographic (gender, age, location, and any other targeting criteria used)

Umniah does provide any details on use of customers' personal information. In section 2.2.2 and 2.2.3 of the "Terms and Conditions" published on its website, the company merely says, "The information and/or material you provide is fit for publication and you hereby indemnify the company if any third party takes action in relation to the information and/or material you submit." It adds that "you warrant that the company may publish the information and/or material you submit and/or make use of it or any concepts described in it in the company products or services without liability and you agree not to take action against the company in relation to it."

Umniah's declaration that it can publish or use customer information for any service or product gives the company maximum leeway. The phrase "fit for publication" is a cause

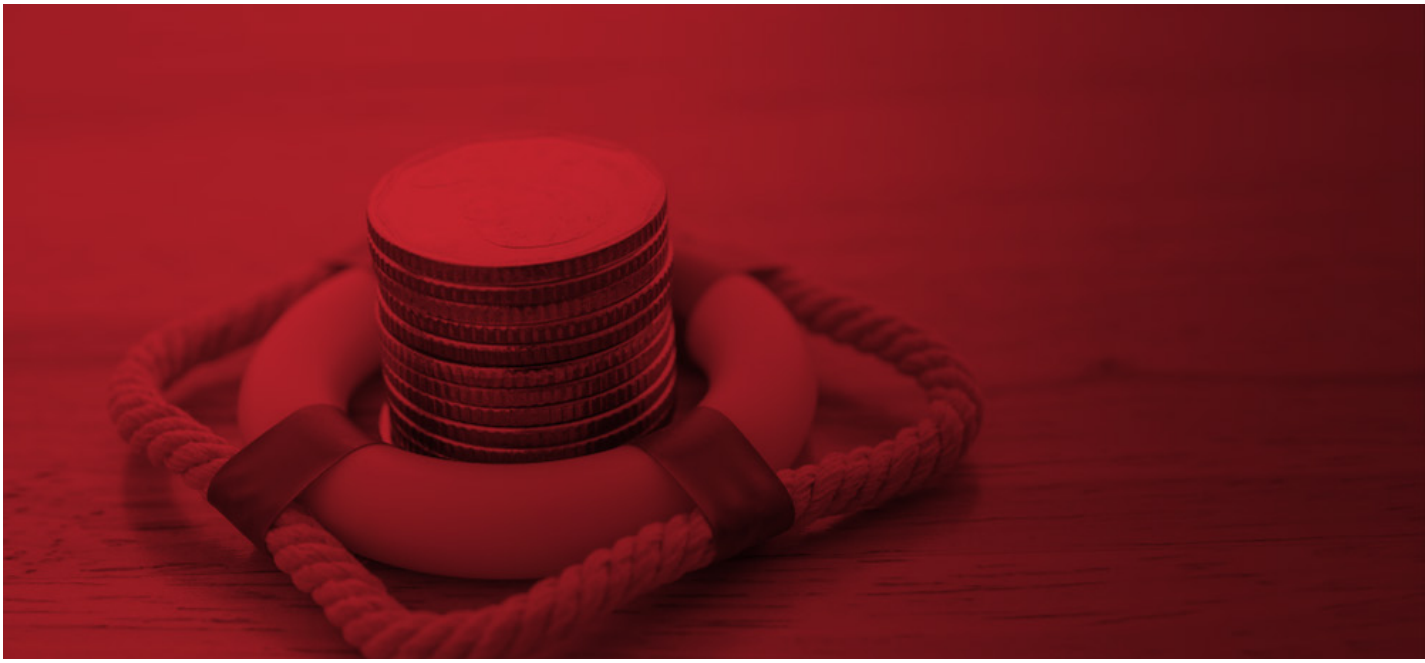
for concern about the extent to which the company respects the data and limits the third parties that are considered suitable recipients. In other words, this could be understood as if the company is trying to run away from its legal liability and responsibility of its obligation to protect personal data and the right to privacy of customers.

Orange, Damamax and TE Data do not offer any details on this issue, which triggers deeper concern about where and how the companies use customers' personal information.

Customers' right to compensation

None of the privacy policies of Zain, Orange, Damamax and TE Data address customers' right to compensation if their rights are violated.

In fact, when it addresses remedies in the case of violation, Umniah does what it can to shirk its obligation to compensate customers, saying, "If you do not agree with this policy, or you are not satisfied with the site and/or services, or you have any claims whatsoever against the company in respect to the site and/or services, your sole and exclusive remedy under this policy is to discontinue using the site and/or services."



Sharing of customer information with third parties

Zain addresses with whom it may share customers' personal information, but is broad and ambiguous, saying "We enter into agreements and business relations with other companies and trusted third parties. These companies can be content providers, solution providers, business partners or otherwise." The phrase "otherwise" allows it to share with virtually everyone.

Orange declares that it may share personal information with third parties but is not specific. It only says this may happen if required to conform with a legal requirement, satisfy a legal process or defend its rights or property.

In its "Terms and Conditions," Umniah does not address if third parties have access to customer information. However, section 5.7 of the Arabic version of its privacy policy warns, "The web is not safe, and while the company tries to protect the website and

services, the user must accept that using or messaging through the website may allow any third party to illegally access his/her personal information. In this case, Umniah is not responsible…"

Both Damamax and TE Data mention the types of third parties with which they may share customers' personal information: security, judicial and other such authorities. They state, "The first party commits to maintain the confidentiality of the second party's information and not disclose them except for information approved to be disclosed from the second party or according to the request of security and/or judicial authorities and/or based on an official request…"

Legal liability

None of the five ISPs agrees to any legal liability in case of unauthorized disclosure or misuse of personal customer information by a third party.

Awareness of privacy policies

ImpACT and Access Now

then prepared a set of questions to assess ISP employees' knowledge of privacy-related issues and whether their companies share user information with third parties. The ImpACT and Access Now teams called the customer-services lines of the five companies and determined the answers to the following questions:

1. When subscribers call or contact them by other means, is their personal information (Name, address, IP address, age, etc.) requested?
2. What type of personal information is collected?
3. Are staff members aware of their companies' privacy policy and whether it is published on the website and/or stated in subscriber contracts?
4. Do the companies employ a personal-information-protection officer with whom customers can communicate and file complaints?
5. Do staff members know if their employers share personal information with other parties, such as other service providers and partners companies? Is subscribers' personal information transferred across borders?
6. Do they inform subscribers who contact them that their personal information may be shared with other parties and if so, their identities?
7. Do staff members know if their companies compensate subscribers in the event of loss, mistaken publication or theft of personal information?
8. Do their employers inform subscribers on their websites or in contracts who is responsible for protecting personal information?

When interviewed in a straightforward fashion as ImpACT and Access Now researchers, staff of two of the ISPs refused to answer, claiming that doing so requires long administrative review to get approval. Accordingly, ImpACT and Access Now team members called posing as potential customers.

All staff members interviewed were aware of the need to verify callers' identities before providing any information on their account. However, they did not answer most of the other questions.

In addition, the ImpACT and Access Now teams contacted company staff responsible for new subscriptions to inquire about privacy issues. Some stated that their companies have strict regulations to protect customer privacy, while others were uncertain and said we needed to talk to someone else about these matters.

Consumer knowledge about privacy protection

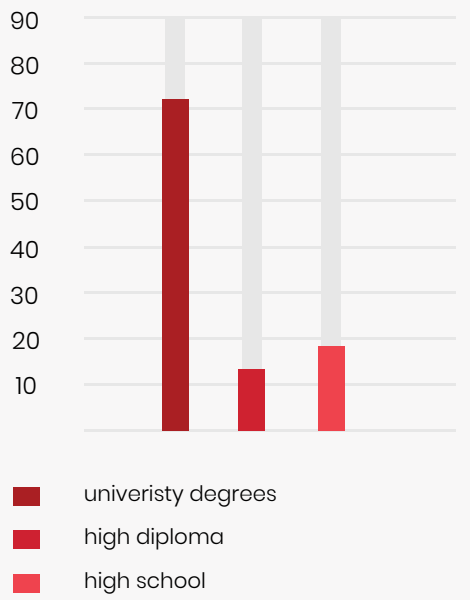
The ImpACT and Access Now teams then set out to assess the public's awareness and understanding of privacy-related issues. A survey was published using Google forms and disseminated using WhatsApp, Facebook and email to journalists, students, employees and activists. About 900 responses were received.

After requesting respondents' age, gender and educational level, they were asked to agree or disagree with the following statements, using a scale of 1 to 5 (with 5 corresponding to totally agree, 2 meaning do not agree a tall and 1 representing "don't know").

1. When calling my ISP customer service number, I am asked to submit sensitive personal information (such as credit card number, ID number or bank account) over the phone.
2. I know the importance of the personal information I supply to my ISP.
3. When I inquire about a specific service, my ISP checks my identity to protect against fraud.
4. I am aware of the law in Jordan regarding privacy protection.
5. I know which official authority enforces privacy-protection rights in Jordan.
6. I am aware of whether I have a right to compensation in the event that my personal information kept by my ISP is lost, stolen or leaked.
7. I am aware of the procedure to follow in the case of fraud.
8. I am aware that the personal information I give an ISP could be shared with other parties.
9. I am aware of the identity of any third party that receives my information.
10. I am confident that the third parties who receive my information will abide by the privacy-protection law in Jordan

Demographics:

Most respondents were young, but of legal age (17-25 years old). Just 25.6% were older than 25. The gender of the respondents was almost evenly split: 55.8% females and 44.2% males. The majority (71.4%) reported receiving universes degrees, while 11.6% had earned a high diploma and 17% had stopped education at high school.



Requests for personal information:

22.1% of respondents stated that their ISP routinely asks them for personal information, 39.2% said this occurs only sometimes and the remaining 38.7% said this never occurred. at high school.

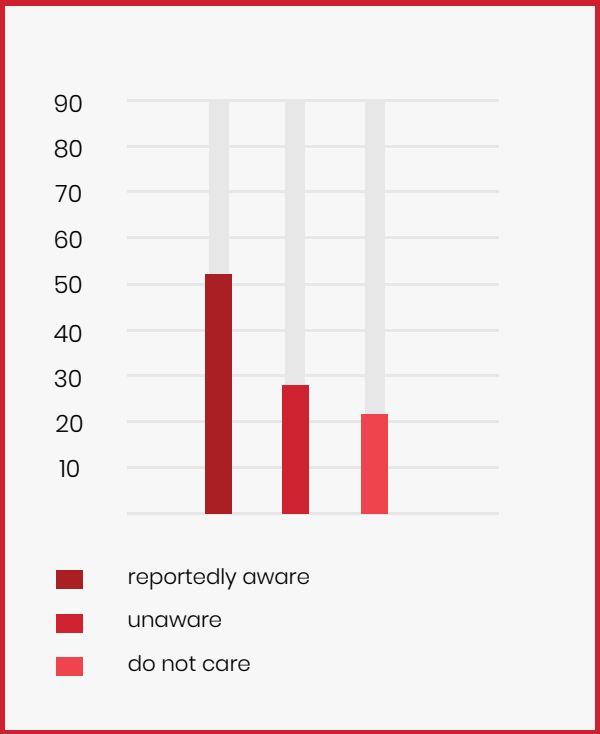
routinely asked for personal information

sometimes asked for personal information

never been asked for personal information

Importance of personal information:

51.3% of respondents claimed to know the importance of their personal information, 27.1% did not and 21.6% indicated they did not care (Figure 2). In other words, more than 48% of respondents either did not know the importance of their personal information or did not care about it.



Fraud protection:

Slightly more than half (52.3%) of respondents said ISP staff always verify their identity to protect against fraud; 29.6% said employees usually do; and 18.1% said precautions are never taken.

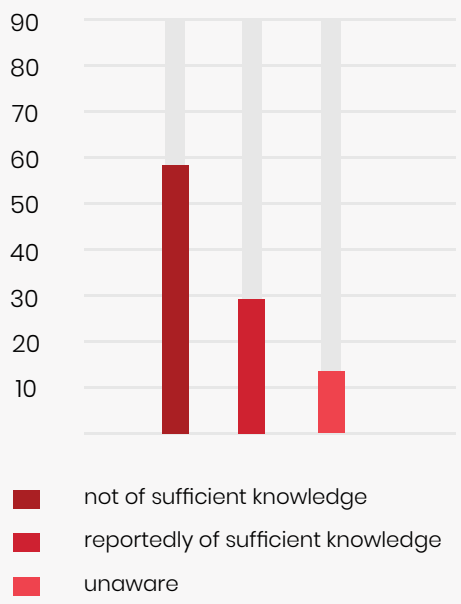
identity always verified

identity usually verified

identity never verified

Cybercrimes, privacy protection and regulations:

Almost 60% (58.8%) of the respondents stated that they heard about privacy-protection law but did not know much about it. Another 28.6% claimed to have sufficient knowledge. The remaining 12.6% were uninformed. Thus, more than 70% of respondents either did not know or did not have sufficient knowledge about the laws that protect their privacy



Knowledge of enforcement authorities:

Slightly more than a half (51.8%) of respondents do not know who is responsible for enforcing privacy laws, 28.1% were aware and 20.1% were not sure.

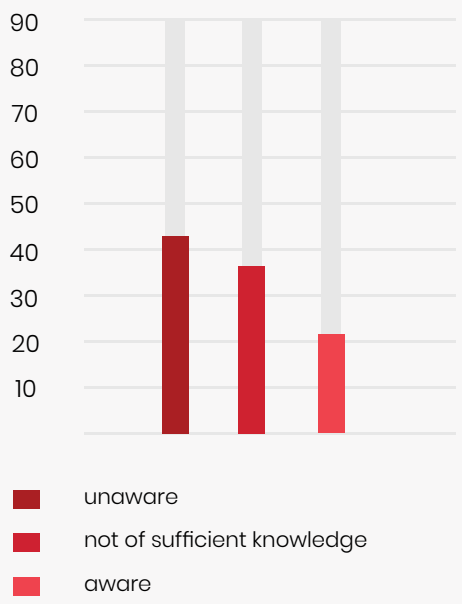
unaware

aware

uncertain

Rights to compensation

43.2% stated they do not know what their rights are if theft or loss of personal information occurs. Another 36.2% knew they have rights but were not sure of the details, and 20.6% reported being informed about their rights.



What to do in case of fraud:

Only 8.1% of respondents said they would know what to do in case of fraud it; 55.3% did not know, 22% thought they knew but were not certain, and the remaining 14.6% said they would need legal advice.

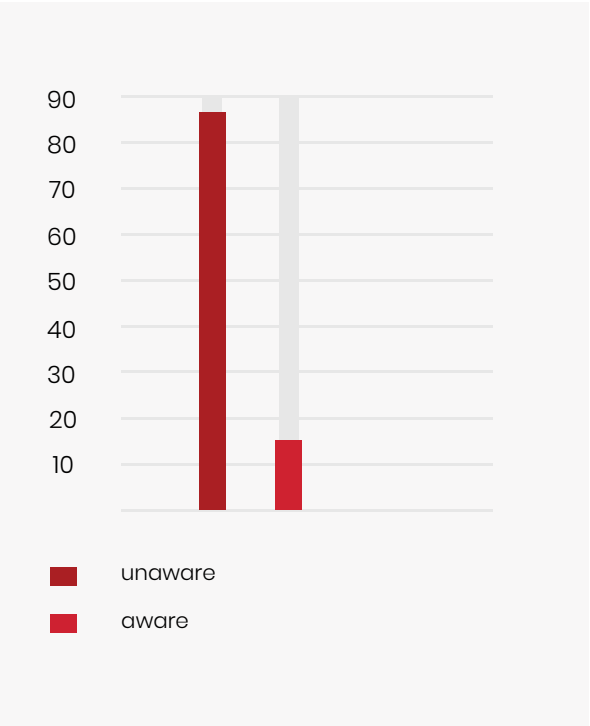
aware

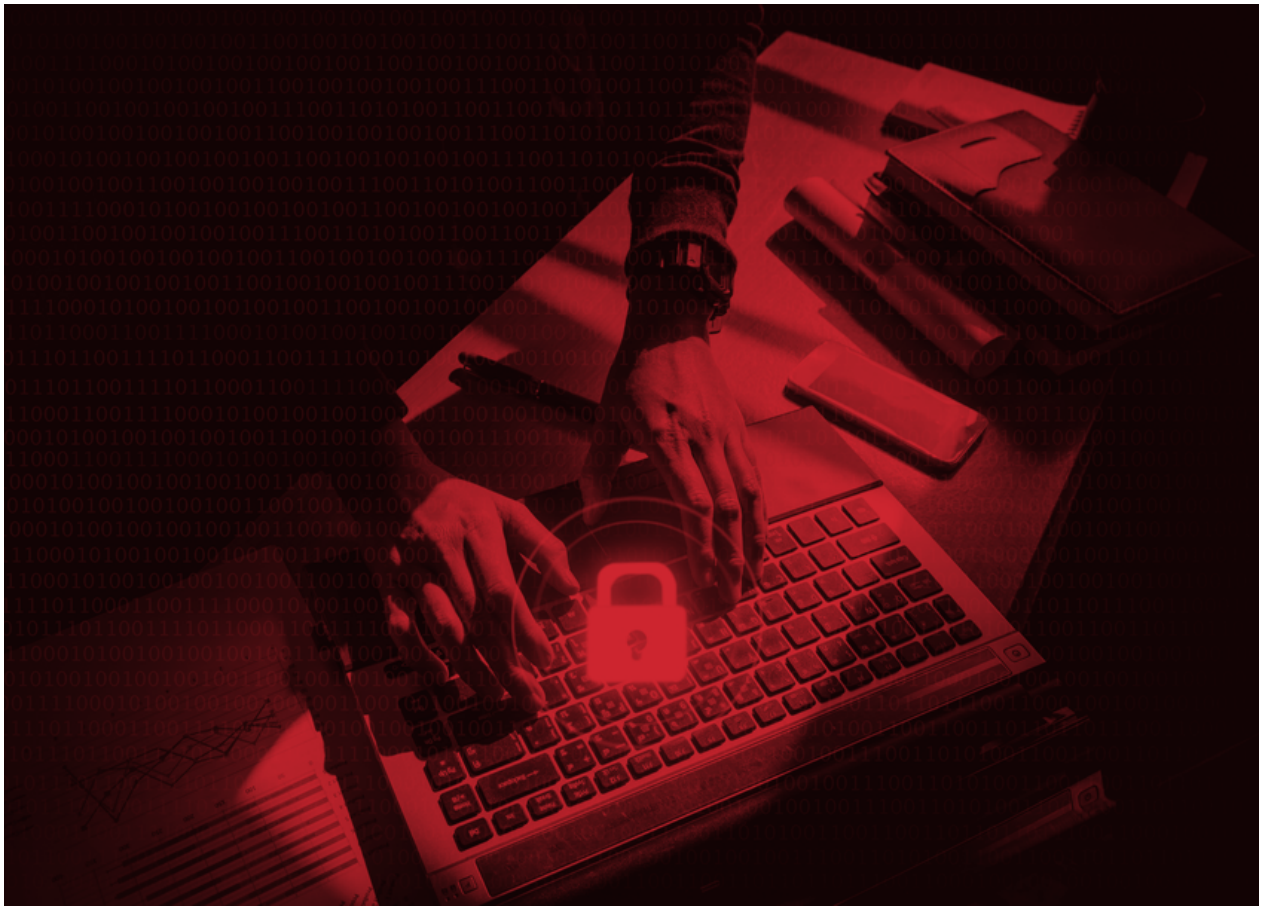
unaware

need legal advice

Awareness of third parties

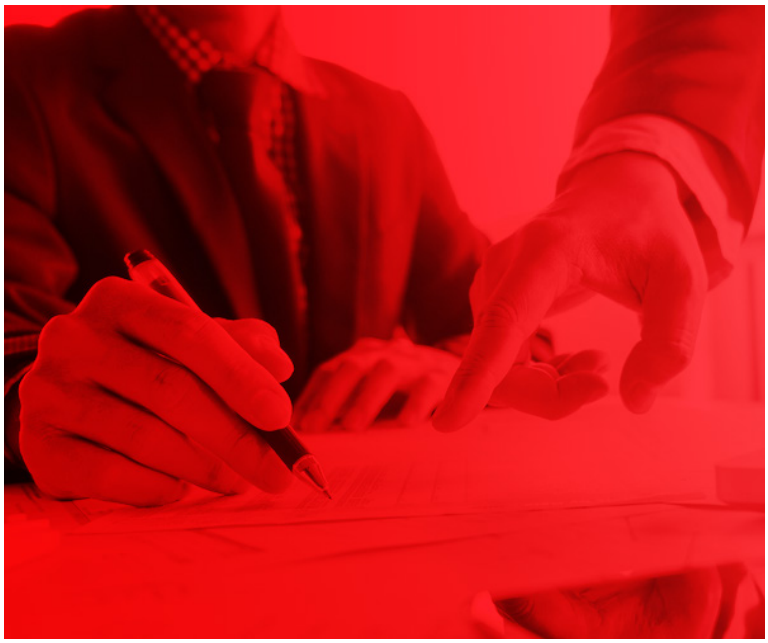
Most (86.9%) did not know who else received their personal information; only 13.1% were aware. Consequently, more than 92% of the respondents are not confident that any third party that receives their information will abide by the privacy-protection law in Jordan.





Recommendations

ImpACT International for Human Rights Policies and Access Now conclude that none of the ISPs examined in this study fully respect and comply with human rights principles and that the privacy policies of Jordanian ISP companies must be modified to address the revealed shortcomings. Specifically, they must include:



- Clear explanations of the personal information collected, and who uses it, where and how.
- A statement also must be made about whether any of this information is shared with a third party and for what purposes.
- The legal liability of that third party must be defined, along with the customers' rights to compensation in case of loss or theft.

In addition, it is clear that currently, most ISP customers are not aware of their privacy rights, the extent to which those rights are being respected or what legal remedy they have if fraud is discovered.

These findings point to a need to educate all ISP customers to protect against the abuses that can and do so easily occur.
Moreover ISP companies process personal data of not only Jordanians but also EU citizens in Jordan. This further means that these companies should comply and be subject to the GDPR (General Data Protection Regulation).

Furthermore, the Jordanian government must prioritize implementing the data protection draft law, to provide adequate guarantees for personal data and the right to privacy of individuals, in order for ISPs to comply with the national and international standards of the right to privacy.

Special Thanks to:

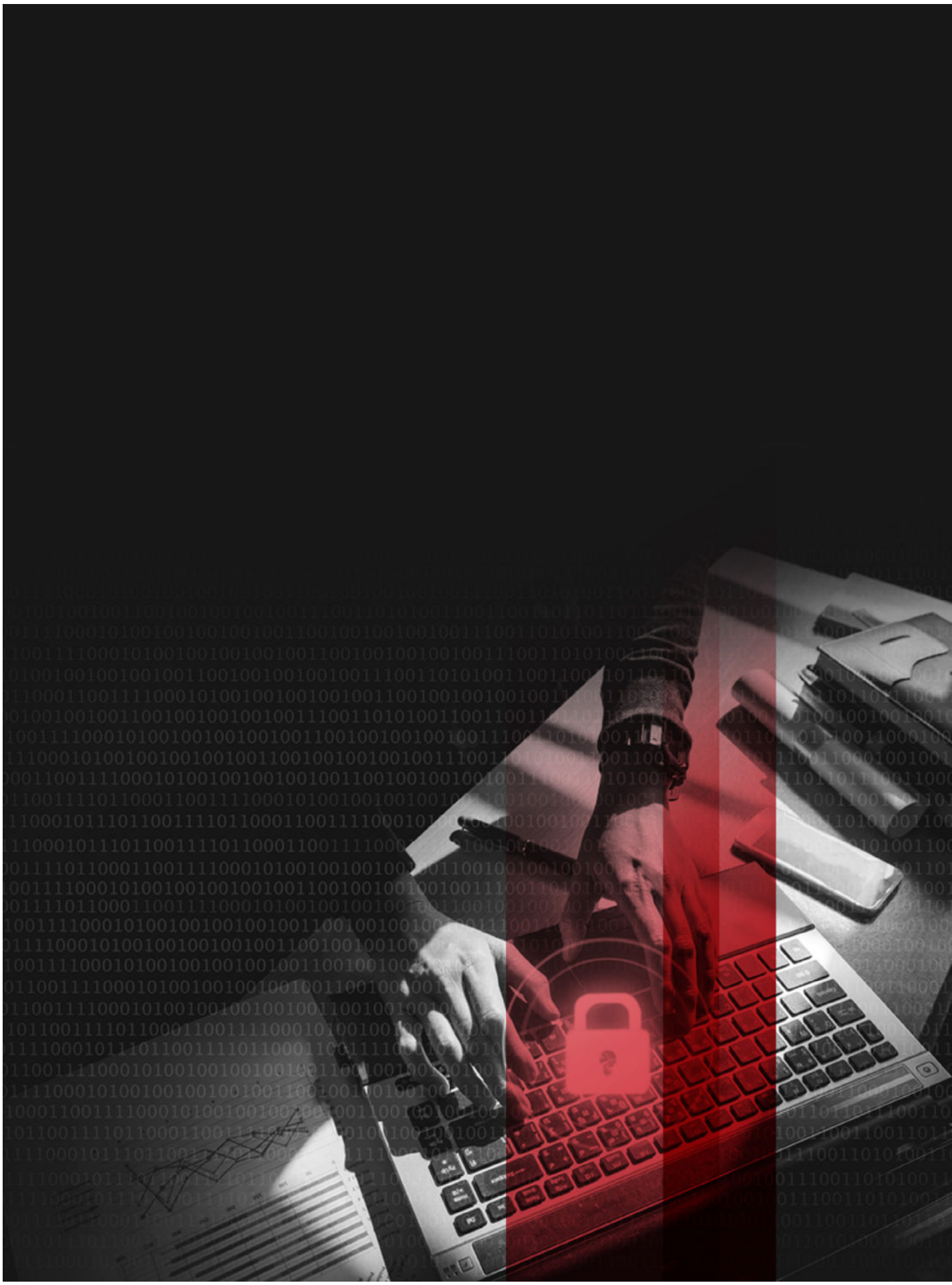
Dima Samaro
MENA Policy Associate

Sami Zeno
IT Specialist

Lara Hamidi
Researcher

Pam Bailey
Editorial Adviser

Laura Hayek
Researcher

Emad Hassan
Designer

Khalil Agha
Digital Media Advisor