Digital Privacy in Jordan

Perceptions and Implications among Human Rights Actors

CYBER STEWARDS

KING HUSSEIN FOUNDATION مؤسسة الملك الحسين
مركز المعلومات والبحوث
INFORMATION AND RESEARCH CENTER

Table of Contents

I. Executive Summary 4
II. Introduction 6
III. Privacy: A Debated Concept 8
a. Legislation: Digital Privacy in the International Arena 9
b. Digital Privacy in Jordanian Legislation 10
V. Methodology 13
VII. Research Findings 16
a. What Needs Does the Internet Serve? 16
b. Do Private Digital Zones Exist? 17
c. What Behaviours Can Protect Your Digital Privacy? 23
d. How Should the Law Protect Your Data? 26
VIII. Conclusion: 29
Appendix I: Interview Questions 32
Appendix II First-and Second Second-Hand Stories: 33

Acknowledgements

This research is a collaborative effort between 7iber Information and the Research Center of the King Hussein Foundation (IRCKHF). Special thanks to Lina Ejielat and Thoraya Rayyes for providing comments and guidance, and all participants who gave their time to be part of this study. This research was undertaken as part of the Cyber Stewards Network (The Citizen Lab - University of Toronto) and supported by the International Development Research Centre.

I. Executive Summary

Edward Snowden's revelations set off a global debate about how states and the private sector should protect the "right to privacy" in practices of access, sharing, and manipulating digital personal data and citizens' private communications. International civil society and nongovernmental organizations called on states and private companies for better legislative protection of privacy, transparency of access and storage, and manipulation of private data. Technical international groups have also debated the possibility of protecting communication and personal information through making the network private by design.

In Jordan, a state with a population of seven million and a 73 percent Internet penetration rate, "the right to private communication" is constitutional. While little information is available on data access and sharing practices among telecommunication companies and government agencies in Jordan, conventional knowledge that "someone is listening in" has always existed among citizens. Despite the anecdotal scattered stories on official interception of phone calls and emails, the debate over legislation of privacy and data protection is still in its early stages because of a lack of documented evidence on data collection and sharing practices. This qualitative research project is the first attempt to investigate the concept of digital privacy in Jordan by capturing the perceptions, behaviours, and experiences of people working in the human rights field. It aims to demonstrate the community's understanding of digital privacy, behaviours to secure communication, and participants' vision of a fair legislative framework that will protect their constitutional right to privacy. We consider the following research questions:

- To what extent are different human rights actors in Jordan conscious of the concept of digital privacy? What constitutes digitally private zones for them? What factors facilitated the formation of these perceptions?
- How have these perceptions affected their communication behaviors and their use of the Internet and social media networks?
- What are their perceptions of the legitimacy and regulation of third parties accessing information online?

Main Findings

- **Despite participants' suspicions about the security of different communication media, the Internet is considered a vital tool for human rights endeavors.**

  The Internet for human rights actors still serves as platform for mobilization, activism, public awareness, and outreach to victims. However, actors' main concerns involved exposing their sources who request anonymity and being blackmailed by personal information available publicly or privately.

- **Human rights actors' perceptions of possible private digital zones are highly dependent on the larger political context in Jordan, according to their individualized experiences and technical awareness.**

  Activists, lawyers, and NGO workers' perception of possible private digital zones in Jordan were influenced by one common factor: the reality of the corresponding political context in Jordan at the time of research. Participants' awareness of the tight institutional and legislative environment to practise freedoms, compounded by the lack of transparency and law enforcement, made them question the possibility of private digital zones. While such absolute private zones did not exist for

participants, imagining "safer" spaces was influenced by highly individualistic and contextual experiences.

When it comes to users' knowledge of available personal information online, visibility, for all participants, meant availability. The information they perceived as being available included all visible posts, pictures, published work, and so on. However, none of the participants mentioned nonvisible data such as meta-data or their navigation history, for example. The limited technical knowledge of online trails formed their perceptions of what should be protected.

- **Participants believe that official entities have the most access to their personal private data and communication.**

  While companies and different online groups were mentioned as third-party entities who might have access to their information, it was not as concerning to participants as official entities' access. Most participants listed the Intelligence Department as the entity most likely to threaten access to their private communications.

- **Perceptions of surveillance do not translate into the adoption of security tools. Self-censorship and conscious selection of communication tools are how users attempt to protect their privacy online.**

  Very few users used information security tools like PGP mail encryption and Tor (anonymity software). Protecting data meant not making it public or sharing it electronically, rather than securing it with technical tools. For example, the more politically active the participants were, the less personal information they shared on social media platforms. When it comes to protecting the information of others, journalists and NGO workers used more drastic measures. They either changed their communication behaviour through choosing a face-to-face interaction when handling sensitive information, or concealed or erased any traces of their sources' names on their devices.

- **For participants, regulating the protection of digital privacy was regulating "surveillance."**

  Participants' views on suitable legislations to regulate access to personal information consolidated with their perceptions of entities that they found most violating. Participant suggestions for a regulatory framework did not go further than the regulation of official entities' surveillance, especially in the name of terrorism. These findings should be understood within the context of the time period of this project. This research was conducted during a period when human rights activism faced a general setback in the rise of a post-2011 revolution's turmoil across the region. While the global debate is turning its focus to violations of privacy within official and private entities, we find that concerns about privacy in Jordan correspond with perceived short-term threats. Private companies' collection of data concerned some participants, however; the vast majority were more concerned with official access to and interception of data and communications. Human rights actors' consciousness of digital private zones, and the security of their communications and data, are therefore highly influenced by the direct threat that they perceive in the lack of legal protection for their rights. In the absence of an environment that encourages free and independent media in Jordan, and with the Right to Access Information law stagnating, participants' anecdotes of first-hand privacy violations can serve as the first evidence of data access and sharing practices among official and private companies in Jordan.

II. Introduction

The right to privacy has long been recognised as an inalienable human right. The Universal Declaration of Human Rights stipulates that no person should be subject to any arbitrary interference with his/her privacy, and grants each person the right to legal protection against such interference[1]. The declining costs of technology along with the rising rates of Internet penetration have facilitated the storage, manipulation, and transfer of massive amounts of personal information about individuals on a global scale. More users are depending on the Internet to facilitate their daily social, financial, and political affairs through different tools and platforms. In the same respect, many companies take advantage of the Internet's increasing penetration to develop business models that treat users' information, traits, and behaviours as a product. Many of these models grant access and analysis of users' information and behaviours in return for a free service. The Internet market has also allowed the development of storage, data mining, and monitoring technologies that enable governments to develop a greater capacity to conduct broad-scale invasive surveillance without legal authority or public disclosure. Because the issue of online privacy has been gaining increased attention, the UN General Assembly adopted resolutions in 2012 and 2013 that aim to protect human rights on the Internet.

The revelations made by former NSA contractor and whistleblower Edward Snowden (exposing the National Security Agency's collaboration across different countries with international companies to access, store, and analyze mass data involving individuals' private information) gave evidence of the importance of defining privacy issues in the digital domain. Following the increasing prominence of cases involving breaches of online privacy worldwide, it's become apparent to the international community that certain measures should be taken to define and control the flow and exchange of information in this uncharted domain.

Efforts toward reform in Jordan in 2012 involved one change in the constitution in an attempt to regulate communication interception. However, there were also changes in the legislative framework that legitimized the storage of and access to digital communication and personal information by different administrative entities. Cases of privacy breaches of Jordanian citizens that surfaced in 2010 and 2013 raise the question of whether or not Jordan is on the right path to protecting citizens' privacy online. The literature that examines and conceptualizes the concept of digital privacy among Internet users in Jordan remains scarce. Even after the 2013 Snowden revelations, public debate on the "right to privacy" did not get picked up across civil society.

In 2011, following the wave of revolutions in the region, social networks became spaces for communicating and discussing social and political demands beyond Jordan's conventional safe zones. Two years later as the region fell into more chaos and political instability, Jordan was also affected by a general activism setback that strengthened official discourse about exchanging liberties for "security." People's concerns about censorship are heightened, especially with the current exhaustive measures that the country is taking in the name of maintaining safety amid Jordan's chaotic political instability. At a time when the official grip has been stronger on liberties, and global discourse expounds on the role of private companies and

[1] Universal Declaration of Human Rights (article 12), available at: http://www.un.org/en/documents/udhr/

governments in protecting the right to privacy, this project explores the meaning and importance of digital privacy to human rights actors and oppositional figures in Jordan. In a country where access to official information is very limited, especially about data access and sharing practices of governments and private companies, this research was meant to explore the perception of digital private zones across the community. In the ongoing international discussion around the adoption of secure tools and software, it is important to contextualize how individuals in different fields, geographies, political realities, and personal experiences choose to protect their information and communication channels. The paper aimed to answer the following research questions:

- To what extent are different human rights actors in Jordan conscious of the concept of digital privacy? What constitutes digitally private zones for them? What factors facilitated the formation of these perceptions?
- How have these perceptions affected their communication behaviours and their use of the Internet and social media networks?
- What are their perceptions of the legitimacy and regulation of third parties accessing information online?

III. Privacy: A Debated Concept

The concept of privacy has many manifestations in different disciplines of study. The right to privacy has long been recognised as an inalienable human right. After extensive normative and empirical studies that attempted to define the concept of privacy, scholars have come to the conclusion that privacy "is in disarray and nobody can articulate what it means."[2] This lack of consensus does not mean that privacy cannot be defined, but rather it reflects the complexities of the concept.

In its most basic definition, the Universal Declaration of Human Rights defines privacy as "an area of autonomous development, interaction and liberty, a 'private sphere' with or without interaction with others, free from State intervention and from excessive unsolicited intervention by other uninvited individuals. The right to privacy is also the ability of individuals to determine who holds information about them and how that information is used."[3] While this definition is widely accepted, it follows the "privacy as a right" approach, which is only one perspective on how research has treated this concept. In an analysis of interdisciplinary research that attempted to explore the different treatments of the concept of "information privacy," Smith, Deniv, and Xu found two main approaches to defining privacy. The disciplines of economics, law, psychology, marketing, philosophy, social sciences, and information systems management treat the concept through either a "value-based" or "cognate-based" approach.[4]

The value-based approach considers privacy as a right integral to society's moral system, and attempts to define the lines between private and public spheres. While "privacy as a right" treats information privacy as an absolute right that needs to be guaranteed, its mechanisms of protection are still under a highly controversial debate between the state, the private sector, or the technology developers.[5]

The controversy surrounding the privacy-as-a-right approach started after the growth of online services to which consumers were ready to submit some of their personal information in exchange for financial gains of discounts and free giveaways. Consequently, the notion of online privacy was redefined through an economic approach studying the cost-benefit relationship involved in the exchange of information between consumers and suppliers. The consumer-behaviour perspective started approaching privacy as a commodity.

Cognitive-based definitions of information privacy treat it as a "state" or as "control." The view of information privacy as a "state" defines it as "the state of limited access to a person" or the state of "being apart from others" whereas privacy as control is "the selective control of access to self."[6] Our research takes the "value-based" approach of privacy as a "right"— whether in Jordan or around the world, we believe that decisions users make about the extent to which they share their personal

2 Daniel J. Solove, D.J. (2006) "A Taxonomy of Privacy," University of Pennsylvania Law Review (154, no. :3), pp (2006): 477-560.

[3] United Nations General Assembly, "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue," 17 April 2013, paragraph 22, 6. Available at http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

[4] H. Jeff Smith, Tamara Dinev, and H. Heng Xu, H. "(2011) Information Privacy Research: An Interdisciplinary Review. ," *MIS Quarterly* 35, no. 4 (2011):, 989-1015.

[5] Ibid.

[6] Ibid., 995.

information or communication are influenced by their limited awareness about how it is being stored, manipulated, or accessed by the data-storing entity. Privacy as a commodity assumes that users have full awareness about the cost of disclosing their personal information or communication. As such, it assumes the existence of a certain symmetry of information between the parties engaged in the exchange of information as a transaction. The fallacy of this assumption is evident in the increased global attention paid to issues of online privacy caused by the asymmetry of information between users and online service providers.

Until processes of access, storage, and surveillance become transparent to the public with a solid legislative framework, digital private spaces are more "granted" by data collecting entities than "drawn by" the user. Because the definition of privacy is still contested, people's perceptions of digital privacy are still being surveyed to inform policies and laws regulating digital data protection, communications, and surveillance. According to Bellman and colleagues, cultural values, Internet experiences, and differences in governments' attitudes toward privacy were influences shaping the different levels of concerns about digital privacy across different countries.[7] Other research suggests that users' "awareness" of operations on personal data are the main influencer for their online behaviours. Communicating a transparent privacy policy, asking permission to use data with third parties, and display of privacy notices reduces users' concerns about privacy when it comes to commercial and public entities.8 Other research suggests that users' trust of platforms is the main influence behind the level of concern about privacy. Individuals may be more comfortable in disclosing their information or engaging in commerce if they perceive platforms as "safe" or "trustworthy."

Users' perceptions can also be derived from the nature of their activity and the perceived threat that it poses to different entities. Individuals who do not undertake "risky" social or political activities may feel less concerned about their digital privacy than those who perceive themselves as a threat to social or political authorities. Our research treats privacy as a variable influenced by the present state of culture, awareness, trust, and political environment. Because these influences are always changing, an individual's perceptions of privacy are highly contextualized and continuously negotiated. As Kimmel said, "individuals are continually engaging in an adjustment process in which desires for privacy are weighed against desires for disclosure and personal communication with others."[9]

a. Legislation: Digital Privacy in the International Arena

Privacy and protection of human rights online has have gained increased attention in the recent years. The Human Rights Council adopted "The Promotion, Protection and Enjoyment of Human Rights on the Internet" resolution in 2012. The resolution was sponsored by Brazil, Tunisia, Nigeria, Turkey, Sweden, and the United States and affirms that "the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice."[10] ' In December 2013, the 193 member states of the General Assembly of the United Nations unanimously adopted a UN resolution on

[7] Steven Bellman, E.J. Johnson, S.J. Kobrin, and G.L. Lohse, "International Differences in Information Privacy Concerns: A Global Survey of Consumers," Information Society 20, no. 5 (2004):, 313-24.
8 Smith, Dinev, and Xu, "Information Privacy Research."
9 Ibid., 1002.
10 United Nations Human Rights Council, (2012) "Resolution A/HRC/20/L.13: The promotion, protection and enjoyment of human rights on the Internet " http://ap.ohchr.org/documents/alldocs.aspx?doc_id=20280

the right to privacy. The resolution marked an important recognition of the changing nature of privacy and reaffirmed that "the same rights people have offline must also be protected online, including the right to privacy." To this end, it called upon states to:

- Respect and protect the right to privacy, including in the context of digital communications;
- Put an end to privacy violations by ensuring that national legislations comply with their obligations under international human rights law;
- Establish or maintain existing independent, effective, domestic oversight mechanisms capable of ensuring transparency and accountability for state surveillance of communications, their interception, and collection of personal data.

On a regional level, the Arab Charter on Human Rights, adopted by the Council of the League of Arab States in 2004, and enforced by 2008, recognized privacy as a right in article 17: "Privacy shall be inviolable and any infringement thereof shall constitute an offence. This privacy includes private family affairs, the inviolability of the home and the confidentiality of correspondence and other private means of communication." [11]

b. Digital Privacy in Jordanian Legislation

The legislative framework in Jordan surrounding privacy, surveillance, and online media started changing in 2012. In an alleged effort toward reform, the government offered a list of constitutional changes. Among them requiring a "judicial order prescribed by law" should there be a need to intercept communication. The constitutional change did not transcend into other laws that regulates surveillance. For example, as of the date of writing of this research, the Telecommunication Law still allows the monitoring of communication through both, a judicial, or an administrative request[12].

The Anti-Terrorism law,[13] on the other hand, authorizes the general prosecutor to subject person to surveillance based on "reliable" information that links him/her to "terrorist activities" without any clear language prescribing what "reliable" or "activity" means. New amendments to the Press and Publication Law passed in 2012 made electronic media owners and their staff "subject to intermediary liability" and "responsible for maintaining a record of all user comments posted for at least six months."[14]

Legislation also penalizes the illegal spread of private messages; but penalties are inconsistent across different laws. While the penal code penalizes spreading the content of private messages for not more than three months in prison, the telecommunication law's penalty ranges between a month and a year in prison, or

11 "Human Rights in Arab Countries: Bridging the Gulf." Available at: http://www.humanrights.ch/en/standards/other-regions-instruments/arab-charter-on-human-rights/

12 Article 29 of the Telecommunication Law: "that the licensee should commit to provide the necessary facilities to the competent authorities for the implementation of court and administrative orders that has to do with tracking communications specified in these orders."

13 Article 4 of Anti-Terrorism Law: "If the Prosecutor General received reliable information indicating that a person or group of persons is connected to any terrorist activity, the Prosecutor General can impose surveillance over the residence of the suspect, his movements, and his means of communication."

14 "Blacking out Online Media," Jordan Business 2013, available at http://www.jordanbusinessmagazine.com/features/blacking-out-online-media

100 JOD to 300 JOD. These penalties are only imposed on people whose job is to transfer calls, which excluded public personal in security institutions.[15]

In addition to changes in legislation, new regulations have been introduced since 2010 that pose a threat to citizens' privacy. Since mid-2010, Internet cafés have been obliged to install cameras to monitor customers. Customers also have to give their personal identification information before they use the Internet and café owners have to save users' browsing history for at least six months.[16]As of spring 2015, a draft for a new Data Protection Law is being developed by the Ministry of Telecommunications. The final draft is still under study and has not been shared publicly. According to the ministry, this law aims to complete the legislative umbrella that Jordan needs to open investment in cloud computing and protect citizens' data.[17]

Public Cases of Digital Privacy Breach

There's a distinction between cases in which citizens' privacy was breached and those where other freedoms were breached as a result of surveillance or commercial use of data by private companies. As of spring 2015, there were no court cases for private companies' breach of their clients' information. However, other cases surfaced reflecting the state's surveillance activities on the network. Jordanians started to officially get convicted in court for their private posts or communication starting in 2010.The first case involved Imad al-Ash, a Jordanian college student[18]. In 2010, Imad was sentenced to two years in prison for insulting the King in poem he posted on a forum under a pseudonym. He was released after a royal pardon. The second case involved Ayman Al-Bahrawi who, in 2013, faced charges over a WhatsApp message found on his mobile phone account. He was arrested for insulting certain Arab leaders.[19]

The frequency of such trials has increased after Jordan's decision to participate in the American-led coalition to fight ISIS in 2014, the frequency of such trials has increased. After the 2014 Anti-Terrorism law passed, many Jordanians were convicted in a State Security Court for "supporting terrorist groups using the webWeb." Their crime involved sharing materials produced by the Islamic State group on social media websites. While it is not clear whether the posts of in these cases where "private" or "public," one of them the posters was convicted for sharing material over the chat application, WhatsApp.[20]

15 Article 71 of Telecommunication Law: "Anybody who spreads or releases the content of any communication through public or private networks or views a telephone message by the nature of his job, or records it without legal base, will be penalized a prison sentence for no less than a month and no more than a year, or by a fine no less than 100 JODs or more than 300 JOD, or with both penalties."
Article 384 of Penal Code: "Responding to the complaint of the victim, one is penalized for not more than three months in jail for breaching the private lives of others by eavesdropping, peaking, or any other medium including recording audio. The penalty is multiplied in case of repetition."
Article 356 of Penal Code: "Anybody who spreads the content of a private call within the capacities of his position in the telephony service will be penalized for 6 six months or charged with 20 JODs. (Article 35,6 months or charged with 20 JODs."
16"Amended Instructions to Regulate the Work and License of Internet Cafes and Centers," [in Arabic], Al Dustour, 3 June 2010. Accessed 14 May 2013. http://tinyurl.com/pc67owz.
17"Data Protection Law Draft Soon," [in Arabic], Volt Jo August 2013, available at https://tinyurl.com/nfqvqlw
18 "Court of Cassation confirms Al Ash Prison Sentence"[in Arabic], Ammannet November 2010, available at http://ar.ammannet.net/news/81394
19"Three Jordanian Activists Jailed for Distributing Flyers Associated with Morsi Supporters," IFEX: The Global Network Defending and Promoting Free Expression, 2 October 2013. http://www.ifex.org/jordan/2013/10/02/activists_jailed/
20 "Jordan: Sanctioning Da'esh Members and Promoters with Prison," Al-Arabiya, 10 November 2014. Available at http://preview.tinyurl.com/lxruh8f

V. Methodology

a. Design

We used a phenomenological approach and aimed to investigate a topic that has not been thoroughly researched in Jordan.[21] We adopted a dynamic qualitative methodology that was flexible enough to change according to the needs and the circumstances of the research participants and team. The research took place over a period of eleven months between January and December 2014. It was based on a thorough review of available literature and legislation as well as semi-structured in-depth interviews with people working in various fields in Jordan, including journalism, activism, law, and development.

b. Research Subjects

Initially, we planned to conduct interviews and focus group discussions with the following groups: journalists, activists, "technology enthusiasts," students, nongovernmental organizations (NGOs), and government officials. However, after designing the methodology and taking into account the available time and resources, the research team decided to focus on in-depth interviews with journalists, lawyers, NGO representatives, and activists who have a strong presence online and rely on online platforms and media in their work. We acknowledge that the sample is not representative and individuals were not selected from different points of comparison. However, what the research subjects had in common was the human rights framework of their work and their heavy activity online in their personal and professional lives. While this sample may not be generalizable to Jordanian society, it targeted individuals who we believe are largely affected by issues of digital privacy in their line of work, as well as their personal lives. Such a belief was supported by the respondents' answer to a question about individuals mostly affected by these issues in Jordanian society. We conducted in-depth interviews with a total of fifteen participants. In the following brief profiles of each group, a pseudonym was given to each participant to protect his or her identity.

NGO Representatives (five participants)— participants had a long record of working on human rights issues through their organisations and their political activism on social media outlets. Their activities ranged between documenting human rights abuses, working with refugees, and providing platforms for community dialogue and mobilization. Ibrahim, Amar, Faisal, Muna, and Zeina were the NGO representatives who took part in this research.

Journalists (four participants)—Their work involved covering, researching, and investigating human rights issues as well as political, economic, and social affairs. Some journalists were also bloggers, one of whom blogged anonymously to tackle controversial political issues. Another works in evidence-based investigative journalism. Journalists who participated were Salem, Ali, Laila, and Muhanad.

Lawyers (three participants)—worked on a variety of issues including representing political prisoners, providing pro bono services, and campaigning for social justice. All of them worked on sensitive legal cases and some of them extend their legal and political activism to social media outlets. Rula, Lama, and Mutaz were the participating lawyers.

21 A phenomenological approach in research involves the study of perceptions and experiences from research participants' perspective.

Activists (three participants)—While all participants may be considered activists in their fields, three were heavily involved in activism. Two of them work on national campaigns demanding gender equality as well as political and social justice, and one is an anonymous political activist online. Activists were Batoul, Raya, and Ziad.

c. Data Collection

The interviewing process followed the same style: we approached the participants and explained the research objective to them. Anonymous bloggers were approached through the research team networks. Following their verbal consent, they were interviewed in their preferred location and the interviews were recorded. The research team asked a set of questions in each interview but gave the participants the chance to elaborate on their personal experiences. During the data collection phase, verbatim transcripts were produced following each interview.

The interview guide can be found in Appendix 1 .

d. Data Analysis

While designing the interview tool, we outlined a set of themes that we hoped the interviews would address. In the data analysis phase, we extracted data from the interviews according to the themes that emerged. Keywords were then assigned to all responses, which allowed us to identify broader categories for analysis. For example, we tested if answers of participants differed according to identifiers like their field of work and the gender of the participant were variables that were taken into consideration during the analysis. After each interview was transcribed, the transcript was reviewed by one other researcher. Both the Information Research Center of the King Hussein Foundation (IRCKHF) and 7iber conducted a full review of all transcripts and analysis sheets to maintain the quality and accuracy of the documentation process.

e. Ethical Considerations

Because of the sensitive nature of both the topic and the participants' field of work, the research team ensured that all ethical aspects of the research were taken into consideration. Before starting the interviews, we obtained verbal consent from the participants to record the interviews and use their responses for the purposes of this research only. The research objective was clearly explained prior to the interview. We also assured all the participants that their identities would be kept anonymous so that they are not subjected to any unforeseen harm or consequences as a result of taking part in the research. In the case where the participants gave specific stories and examples, any identities in the stories were also kept anonymous. The research team was also careful in handling the data, namely the recordings, transcripts, and data analysis sheets. Such data were exchanged offline, or online using encrypted emails. No one outside of the research team had access to the data.

f. Research Limitations

This research was exploratory and aimed at probing perceptions and experiences. It is neither quantitative nor representative of vast swaths of Jordanian society. The questions we asked participants working in NGOs differed slightly than those we asked to the rest of the participants. Interviews with lawyers, journalists, and activists aimed to investigate personal perceptions and experiences, while the ones with NGO representatives additionally aimed to explore the privacy of information within the NGOs as they deal with sensitive data. Because the interviews with NGO

representatives asked some of the personal questions as well as more general questions about the NGOs, not all personal questions were asked, given the limits to our time together. We would have liked to conduct more interviews with participants from these fields and others. However, working with constrained resources, we had to be selective in choosing the sample of participants we felt would be the most diverse yet representative of human rights actors.

VII. Research Findings

The structure of the interview protocol and analysis of participants answers identified four main areas through which findings emerged on the the relationship of participants with the internet as a private or a public space, and the perceptions of their digital privacy. These areas were:

1. The functions that Internet serve.
2. Perceptions of digital private zones.
3. Perceptions of behaviors that protect digital privacy.
4. Perceptions on required legal protection.

a. What Needs Does the Internet Serve?

Batoul, one of the activists we interviewed, said, "I am only away from the Internet dcuring my sleep time. Previously, you had to sit somewhere in order to connect, but with smart phones the Internet is now in your bag and pocket." Batoul's statement was typical of many comments our respondents made indicating a similar high reliance on the Internet. Comments such as "I spend 95 percent of my time online," "eight to ten hours a day," and "obsessed with social media," show that, like Batoul, being connected is an essential component in participants' efforts to pursue their personal and professional lives. Batoul's general reliance on the Internet related to her activism communication needs while leading one of Jordan's biggest gender equality campaigns.

The network also served as a safe communication method for Rula's clients. As a human rights lawyer, she found the Internet to be highly beneficial for communicating with clients who wanted to remain anonymous before they could gain trust to hire her. She also said that she used the Internet to raise awareness about court rulings.

> I use the Internet to raise awareness on details of cases that the media either trivialize or exaggerate, like what happened with the "Satan Worshippers" case.[22]. I also use it when a client needs high privacy, and wants to consult with me on a case without revealing his or her identity. They starts asking questions until they gain enough trust to come and meet me face to face. (Rula, lawyer)

Other aspects of the Internet such as its potential to mobilize groups appealed to other activists such like Raya who said "when someone wants to spread the word about a strike taking place in a certain hour, I circulate it to my friends through posting it on our Facebook page, since I cannot contact them via phone during working hours."

Others found the Internet beneficial in researching and mapping news coverage.

> I spend around six to eight hours in total online. It is a very important resource for my work as a journalist, as any kind of research starts online. I use twitter Twitter to spread information about important articles that get overlooked in the state newspapers. For example, reports on Jordan's airplanes deal with Pakistan. (Salem, journalist)

22In February 2013, four university students were wrongfully convicted by Military Court of "worshiping Satan." Identities and misinformation about these students were published across many media platforms. In May 2015 the students were proven innocent.

> My dependency on the Internet for work is 99 percent. As soon as the Internet cuts off my work stops. As for my writing, I rely 85 percent on the Internet. I use it for personal communication—from one to one-and-a-half hours .[per day]. For information sources, I use governmental websites, the central bank, news sites, the *Economist*, and sometimes *Huffington Post*. (Faisal, NGO representative)

The most common social media platforms among participants were Facebook and Twitter. Participants mainly used these platforms for sharing, outreaching, and researching their human rights work. Their use of the Internet for personal communication with family and friends was not as noticeably important.

b. Do Private Digital Zones Exist?

While respondents all have a general understanding of what digital privacy entails, their understandings varied. In the absence of a transparent framework for the mechanisms of access, sharing, and storage of information, respondents' notions of privacy are constructed individually. Individual perceptions are particularly important. The information provided by respondents was mostly in the form of opinions they developed based on multiple factors: personal experiences, technical knowledge, assumptions about third-party access, and platforms' trust factors. While answers were very different on an individual level based on these factors, one commonality that united many perceptions was the political context of the state at the time of the research. This is highlighted in answers respondents gave regarding:

- What personal information is available online?
- Who can access personal information? And for what reasons?
- What is considered to be a safe medium and what is not?
- What behaviors should one follow to respond to privacy-related concerns?

The varying responses to such questions indicate the highly context-dependent nature of individuals' Internet engagement —which result in their perception of digital privacy. The notion of privacy is thus not a binary quality that either exists or does not exist. Instead, it is a wide spectrum of different levels based on surrounding short- and long-term variables.

i. Availability of and Access to Personal Information Online

A section of the questions we asked participants probed their understanding of what information about them is available online. When asked about what they think would be found if one googled them, the respondents' gave different answers that further indicated a spectrum of understanding about their online trails. A majority of the respondents pointed to their political views and opinions. Their personal information was not perceived as available. However, this may pertain to the particular nature of the sample (that is, who they are mostly involved in human rights activism and journalism).

> My character is very much revealed online. Type my name and you will find a million articles or contributions in forums—you might even find my phone number. (Batoul, activist)

> Since I am a consultant and a columnist, some people shared my CV online. You can also find presentations. (Faisal, NGO representative)

> I think you will find my human rights work and reports—there is nothing personal about me online. There might be a picture or two on the organization's website, but I don't think there is anything else. (Amar, NGO representative)
>
> You might find mostly my professional profile on LinkedIn—you'll find my place of work. My name is mentioned in the credits of the documentaries I make ... You might find pictures too. (Laila, journalist)

The answers differed when aspects of personal or private information were the topic of the question, rather than work-related, professional information. Many participants indicated that what personal information is available about them online is only what they choose to share on social networks . For example, Muna believes that she "manages" her private information through privacy settings on Facebook.

> Nobody can see my photos when I apply privacy settings on my Facebook. For example, acquaintances can't see photos of my husband, children, or personal life. There are things that you cannot control, such as general information on my activities through press releases, or people tagging your photos, however, nothing too private as I refuse to subscribe to services that share information like things I read online, for example. (Muna, NGO representative)

The respondents' perceived knowledge of such control is further exemplified by Ziad and Salem, who believe that they have full knowledge of the online availability of their private information because they actively "Google" themselves. What they both have in common is that they share limited personal identifying information online; one of them was an anonymous blogger in the past and the other anonymously manages a Facebook page that mocks political issues in the country.

> I research my name regularly on Google and I can't find anything apart from a few comments here and there. I'll find a few friends. But it would be hard to connect them to me. I've done my best to keep a low profile on the web anyway. (Ziad, activist)
>
> If you dig deeper, you will find four personal photos of myself; three do not look like me now. One of them was posted by a friend of mine on his Geocities page, as we were close friends. My blog won't appear in the results because it is not under my name. (Salem, journalist)

However, while certain people believed they control the flow and availability of their personal information online, opinions of others stood in stark contrast. Such opinions reflected a belief in the availability of "everything" about them online despite any privacy settings. This was demonstrated by respondents like Ibrahim who believe that one can find a lot about a person through social media platforms. "Facebook is a great tool for any intelligence program. It is a program that is 100 percent successful. Through a Facebook account, you can know who the person is, how they think, and their politics, through whatever they share online." (Ibrahim, NGO representative).

Batoul, the activist, believes that "everything" about her is available online. This was also echoed by Laila, who said that one can know everything about her life if they have access to the Internet. Raya added that her political views on certain issues on her Twitter and Facebook accounts are the first thing that one can find about her. She jokingly said:

> “Intelligence officers should only google my name to find everything about me. Why intercept? Everything is public nowadays. I stopped posting all my photos publicly, like I used to in 2011. I still believe that it does matter, as photos were still taken off my private profile. (Raya, activist) “

The (sometimes contradictory) opinions about what information is available online caused us to question how such information is shared. Respondents were asked whether such information was shared voluntarily or otherwise. Once again, a difference of opinion was prevalent. Many participants believed that all the information available about them online was voluntarily shared by them, while almost half of the participants believed that there is information about them online that they did not volunteer to share. Some mentioned things like tagged photos on Facebook.

> Certainly. There are photos of me that people usually share in weddings, trips, and activities. So far I have not seen a displeasing photo... but sometimes I remove tags. (Ibrahim, NGO representative)

> One girl volunteered to use the story that I shared about my daughter online in a video that supported the campaign I am working on. I was not happy and asked her to remove it as it was not for publishing. (Batoul, activist)

Other involuntarily shared information included misquotations, personal attacks, or photos modified for defamation. The research team didn’t strictly define what “personal information” included. This flexibility caused different participants to define the concept differently. While some included work information and political information in the category of personal information, others included only information about themselves and families. This inconsistency reflects an aspect of the difficulties faced when studying the topic of digital privacy and privacy in general. While our approach in addressing privacy as a right attempts to define perceptions of the private and the public spaces, such a definition distinction is difficult to sustain because it is highly dependent on the individual and their particular context. For Aya, Batoul, Muna and Raya, private information that needs to be digitally protected meant family and relationships information. In contrast, to only a few men, highlighting “family information” as information that needed protection. When it comes to profession, lawyers and journalists highlighted information about their clients or sources as private information that needs to be protected.

Similarly, the context in which individuals operate can be affected by how certain they feel about their knowledge of what the trails they leave online. This was largely manifested by the strong correlation respondents expressed between the availability of information and their visibility. The information they perceived was available about them online— including posts, pictures, published work, and so on—, is all visible information, whether on Facebook or Twitter. None of the participants however mentioned the possibility of availability of non-visible data such as meta-data or their navigation history, for example.

ii. Perceptions of Listening Ears on digital Private Data

There are factors unique to the local Jordanian context in which all of our respondents operated that shape their perception of privacy. Recent developments in the legal framework governing the sharing of information were criticized as being restrictive to freedom of speech in Jordan. Such criticized aspects include making website administrators and owners responsible for all content on their websites, including user comments. This scrutiny explains how some would be hesitant to share certain opinions on the Internet. These legal provisions indicate the government's access to such information online, which some might consider illegitimate and a breach of privacy. This legal context results in an air of uncertainty regarding who is under surveillance. As Amar mentioned:

> It's always an outstanding question. We assume that there's some kind of surveillance but we don't know how intrusive it is. I would be shocked if all the ISPs [Internet service providers] weren't handing over all of their data to the government. I mean I don't have evidence to say that they are but I think pretty much in the entire region that's pretty standard. (Amar, NGO representative)

It became apparent that there was a need to investigate the sample's perceptions of who can access their information and why they would access it. A good starting point was to ask respondents whether and what third parties they believe have access to their personal and private information. Almost all participants echoed what Amar said: "One hundred percent I personally feel like my phone, email, and Facebook are tapped and that is why I do not share most of my personal information, just general things". (Ibrahim, NGO representative).

When asked who those third parties were, the participants gave a variety of answers but the most common were (in order): the General Intelligence Department, security apparatus, and government; commercial and marketing companies; Facebook users, and Internet service providers. Raya and Laila mentioned the CIA and the Snowden revelations when they spoke about breach of privacy.

> I don't think somebody is monitoring my phone, but certainly my online activities. I know this through the leaks [Snowden] that revealed the National Security Agency activities in archiving the Internet. I know my information is being stored, but I am not too much of a public figure for it to be used against me. In Jordan, I know that intelligence keeps all your information, but I don't think they are technologically advanced to access all our phones. (Laila, journalist)

> I fear Facebook. I fear the amount of personal information they have about me especially after the Snowden revelations of their cooperation with the CIA. (Raya, activist)

The majority of participants were certain that the local intelligence and security apparatus have access to their personal information, sometimes with the help of telecommunication companies.

> Absolutely, I'm being monitored. Maybe not me personally, but the page. Probably it is the IT department in the *mokhabarat* [intelligence]. Why? Because I think I crossed a few red lines, probably criticizing the king and queen. If *mokhabarat* is monitoring me, they will get the help of the telecommunication companies. I'm not sure if

> Orange will be interested in what I'm doing anyway, as long as I pay my bill. (Ziad, Facebook page admin)
>
> The third party is the government and security apparatus. That's if they are interested. I don't think anyone else is interested. (Salem, journalist)
>
> Of course there is a third party with us on the phones and our profile pages. It is the government and the IT department of the intelligence agency… telecommunication companies hand in all our data to the government. (Raya, activist)
>
> I know that in Jordan, the security apparatus has a direct line with each telecommunication company that will enable them to store his/her calls, monitor his/her phone, and filter his/her emails using certain keywords. Sometimes they store these for a year. (Faisal, NGO representative)

Additionally, many participants referenced private companies as a third party with access to their information for commercial purposes. The private companies included social media platforms, Internet service providers, and social media marketing companies.

> I am sure that my online shopping behaviors are tracked. I know that because the side ads that appear on my Facebook profile are very relevant to my shopping choices. (Muna, NGO representative)
>
> Commercial companies keep track of your orientation and interests so that they categorize users and customers. (Lama, lawyer)
>
> Social media companies access your tweets to measure the public mood towards certain issues. (Laila, journalist)

The other commonly mentioned third-entity was individuals on social media websites with attempts to defame a politically active participant through keeping screenshot archives of activists' posts or photos.

> Nowadays those who disagree with you politically try to document everything you say through keeping a screenshot that they can use against you later. (Lama, lawyer)
>
> Sometimes I post things that people disagree with. Three months later, a screenshot of that conversation comes up to discredit me in another conversation that is totally irrelevant. (Muna, activist)

The respondents unanimously agreed that third-party access to their information took place. A large majority of respondents believed such third parties to be the government's security and/or intelligence apparatus such as the General Intelligence Department. Other third parties such as private companies were also named, but to a noticeably smaller extent. Drawing on our previous legislative review it appears that while private companies might have access to private information online, the respondents prioritized governmental entities to be the biggest threat to the privacy of their information. Such a perception may be largely a result of the sample's composition and the nature of their professions. Regarding who they believed to be most vulnerable to breach of privacy, respondents' answers varied in ranking people. The most commonly mentioned individuals were activists, public figures, and

opposition views. Ibrahim noted that

> "it's the people who are challenging the status quo—who are trying to do something different. They might have social or political agendas and have some kind of activity in the public sphere. I feel that people who are most vulnerable are activists and members of political parties. "

To understand why such groups are likely to be the most vulnerable, respondents were then asked about the information that third-party entities are likely to seek and how they would use them. Participants identified political opinions, writing, emails, conversations, and contacts.

> Written scripts, pictures, and collected documents for an investigation I am still working on. You know, when we are working on investigative journalism, we do not disclose the information that we have immediately, and we wait until our information is complete. There was an investigation that I was working on for a year. They got a hold of the data that I have—and did not want to share with anyone—and discussed it with me. (Ali, journalist)

> They care about your connections and the type of your relationship with certain people. Also, your political opinions toward certain issues. (Laila, journalist)

> They would probably like to know the identities of the people I am talking to on specific issues. For example, if I'm working on a specific issue, the intimidation wouldn't come on me. I wouldn't hear anything but the person I'm corresponding with would. Somebody would get to them and say to her you better be careful, we can do things to you, we can… so that happens occasionally. (Amar, NGO representative)

Other answers included private information such as family relations and marital status. Lama spoke about a first-hand experience:

> Social media might like to track users, especially people who have influence. For example, Orange sent me a cupcake on Mother's day. I am sure my name is listed somewhere, maybe I'm on a list of influential people on Twitter in Jordan. When they sent it [the cupcake], primarily they knew that I am a mother, which must have taken them some effort to find out. Not only that, but they also knew where I worked and called me, which means they have access to my information. (Lama, lawyer)

The answers respondents gave regarding who is most likely to be vulnerable to a breach of privacy, by whom, for what information, and for what purposes indicate aspects of the Jordanian context. The third parties were mostly described as governmental entities targeting people "challenging the status- quo," more particularly information regarding their intimate personal relations with family and friends for the sake of blackmail, surveillance, harm, commercial use, and limiting people's freedom.

> For the purposes of surveillance, control, applying pressure, and as a scare tactic. All of these may be tools to impact the freedoms of people after all. (Ibrahim, NGO representative)

> In a country like Jordan, the worst nightmare is blackmail. For

> example, a text you are sharing, an email, an intimate relationship ... I try to remain anonymous as much as possible, but I'm not obsessed with this issue. This is how the apparatus works— they want you to keep thinking about it and to self-censor as a result. (Salem, journalist)

After the application of the Anti-Terror law in 2014, many citizens were legally held accountable for private messages through communication apps like WhatsApp by searching their devices according to their lawyers[23].

While there was no precedence mentioned for citizens taking legal action based on illegally accessed or surveilled information, there were abondant examples of court cases initiated by the public persecutor against private messages on chat applications and social media platforms[24]. Certain activists and lawyers were more comfortable talking about the threat of blackmail and possible defamation by individuals who have opposing views, particularly political ones:

> I might post something that not all people agree with. Two or three months later, they post a snapshot of what I posted and throw it back at me for the purpose of discrediting me. (Muna, NGO representative)

> Being a woman in a conservative society, they used my picture to intimidate me through desecrating my reputation. (Raya, activist)

> When I started getting to know my husband, before we got married, a photo of us was uploaded on a "loyalist" Facebook page, claiming that he got me pregnant. Also, when my husband was in prison, people online started talking about the private details of our lives as if it was a soap opera. They call me on Twitter the "Bride of the Roundabout" because I met him in demonstrations. (Raya, activist)

Considering how perceptions and impressions stand at the centre of this research, the participants were therefore asked if their impressions were a result of first-hand experiences or stories heard. Fourteen of the participants were asked this question with more than half stating personal first-hand experiences and the majority saying that their impressions arose from stories they heard from friends and colleagues (see appendix II).

c. What Behaviours Can Protect Your Digital Privacy?

Perceptions of privacy-protection possibilities are formed through a multidimensional construct. Users' actions to protect their information depend on which entities they perceive have access to that information, and the immediate opportunity cost of sharing or communicating. Being outspoken activists, human rights lawyers, and journalists, they narrowly confined their definitions of third parties to official entities, and "nationalistic trolls."

The more information individuals have on the usage or the collection of their personal data by public or private organisation, the more aware they will become about their privacy.[25] Our research sample learned about third-party entities through first-hand stories of hacking and interception attempts. Participants made active choices to protect their information, influenced, first, by their limited technical awareness of

23 Almasri, R. "Anti-Terrorism Law: between the persecution of terror discourse and oppositional opinions" 7iber Dot Com 2015 17 July 2015. "http://www.7iber.com/2015/07/charges-under-anti-terrorism-law-jordan/"
24 Smith, Dinev, and Xu, "Information Privacy Review" 2011."

data access, storage, and manipulation, and second, by a perception of the possibility of gaining control over information using available "security" tools. In this research sample, participants resorted to three main behaviours to secure their information:

- Securing passwords
- Changing communication behaviours
- Limiting usage of communication tools

i. Securing Passwords

Lack of knowledge about platforms' utilization of personal data and the implications of sharing reduces security practices to simple practical steps. One third of the participants trusted certain platforms and either changed their account passwords regularly, or used their offered "privacy" features to protect their information. Those who experienced hacking continuously changed their passwords: "I used two-step verification on Facebook because my account was hacked several times." (Raya, activist); "I change my Yahoo password frequently every three months" (Rula, Lawyer). '

People's trust in changing passwords as the only tool to protect information and accounts arise from limited awareness about hacking methods. Although, the lawyer Lama had been subjected to many hacking attempts, even after setting complex passwords, she only resorted to only two-step verification to protect her information. She explained:

> "I learned to secure my Yahoo account through sound verification and through using complex passwords that are irrelevant to my personal information."

Trusting the medium also means trusting the features it offers to protect privacy and the "feeling" of control over personal information. Those who saw Facebook as a safe space, use its "privacy features" to minimize the extent to which their information can spread, without giving attention to how the medium itself can use their information, or continuous changes that these companies make on their privacy policy. Almost half of the participants saw that different features on Facebook make it safer to use. They cited limiting their audience on Facebook by using closed groups and not pages, private messages, and limited posts. "First I categorize my friends. I don't let my personal and family photos be accessible to all friends because I don't know them well, or I don't trust them. " (Lama, lawyer).

Awareness of interception does not translate to an active continuous plan to protect information. Many participants lived through a "privacy paradox" where their stated concerns of privacy led to actions only when perceived threats were immediate. Even after the journalist Muhannad was subjected to a first-hand privacy violation, he still shared his laptop with strangers, knowing the risks of doing so:

> "I used to be careless, but after what happened in my institution, I started changing the password every once in a while. I also started controlling my friends' lists on Facebook and followers on Twitter. However, I still let random people at work use my laptop, and it is easy for them to access my pages. " (Muhanad, journalist).

This also applies to Ziad, the anonymous Facebook page administrator who said that he is not doing enough to protect his identity, despite how controversial his page is.

His only measure of security is a very secure password to a non-active email: "The email connected to my profile page has no relation to my identity. I never give it away, so you could never log in or try to log into a profile unless you know the email. Once you know the email, you could try to figure out the password … I am not using enough protection online, so it's easy to find out who I am. " (Ziad, activist).

ii. Limiting the Use of the Mediums

Participants took more measures in protecting information that they hold about others than in protecting their own. Both journalists and human rights activists displayed such attitudes. Actions aiming to protect the information of others was part of a well-thought-out plan that mainly reflected distrust in the medium, or perceptions of higher interception technologies.

Amar, for example, attempts not to send any of his documents through email, but rather resorts to a physical exchange of files:

> So I have been working on one particular issue recently, the treatment of Palestinians from Syria, and that research is very sensitive and the people who talk to me are at the risk of deportation, all of them. So for that we actually just did it all on paper—we don't have anything electronic. So to contact them I used a third phone not registered to me so we can find a place to meet and I had my phone switched off the entire time. And I have been seeking input from various organizations that know something about this, so that if I did give them an electronic file it's on a USB stick and I'm handling the paper copies but there's nothing over email. (Amar, NGO representatives)

For some journalists, protecting their sources meant not contacting them by telephone as much as possible:

> I protect my sources through cutting all contact with them without any exception. (Ali, journalist)

> I save my contacts in pseudonyms, and sometimes, I do not store their numbers at all. I only contact them via phone if it is not an emergency, with a prearrangement not to exchange any information via phone. Deciding on a location to meet and exchange information is the maximum use of a phone call with my sources. (Laila, journalist)

The knowledge of online messages' technical mobility contributes to informed choices that some participants make in choosing one platform for communication over another:

> If someone wants to send me sensitive information, I would ask them to do it over Gmail rather than Hotmail or Yahoo … Gmail to [organization] server would also be secure because that transaction would be happening inside the United States between Gmail servers—the communication would only be in the US. So the only threat is if the US government got the information and shared it with the Jordanian government. (Amar, NGO representative)

Those who did not have any trust in any digital medium, and therefore no trust in its so-called privacy features, believed that controlling their information can only happen by preventing it from getting to the medium in the first place. Answering to the question of "how do you protect your data" some answers were at a contradiction

with the "trust" that participants expressed of certain platforms. While some participants believed that Facebook can be a secure space, the majority of participants reported actively refraining from sharing personal photos or information about the family and their activities on social media platforms, mostly referring to Facebook and Twitter.

> Just two years ago, I used to share my health information, travel details, family celebrations, and photos of my children. What did not change is sharing my political commentaries. Before it used to be too public and I never thought about who reads it, or what reactions it would generate. But when I nominated myself for election, I got a feeling that I need to draw a line between the private and the public. (Muna, NGO representative)

Although, his choice for anonymity for Salem, the journalist and ex-blogger, had nothing to do with privacy, he stopped sharing personal information on Facebook or his blog after he revealed his identity.

> When you Google my name, my blog won't appear in the search results because it was not in my name when it was active. Nowadays, I only update it three or four times a year to publish an unapproved article, or to vent something that I do not wish to share on Facebook. The blog was not under my name simply because all bloggers in that period [2007] were not writing under their names. It had nothing to do with privacy. The focus was more on the content than the person behind it. It was not for security reasons. There are bloggers who remain anonymous up to this date ... You are a lot more comfortable with sharing personal issues when your identity is not revealed. Revealing my identity has affected my ability to write about personal issues on my blog. (Salem, journalist)

Even after one Lawyer expressing how Facebook was a safe platform to talk to some of her potential clients, she decided to deactivate her account altogether after journalists turned her posts into news pieces taken out of context without her knowledge.

The privacy protection measures adopted by respondents differed widely and were at times inconsistent. This was highly dependent on what they perceived to be vulnerable information, and who they thought would want to access it and for what purposes. While the participants were selected because they were generally active online in their professional capacity and handled sensitive information, very few used complex measures to protect their privacy despite the nature of their work. For example, none of the participants used PGP encryption tools. There was a general acknowledgment that they did not do enough to protect their information online. And those who were very vocal on Facebook and Twitter about their political opinions and views tend to share less or avoid online personal details all together. They held a spectrum of different opinions regarding the possibility of privacy on the Internet. Some individuals believe they can protect their data, whereas others completely rejected the idea of such privacy being possible.

d. How Should the Law Protect Your Data?

Two schools of thought have emerged when it comes to entities protecting the right to privacy. Scholars who define privacy as a commodity that users exchange in return

for services place the right of protection on the private market. This camp assumes that users have access to clear knowledge on access to and usage of their data. It also assumes users' rational choices in disclosing information, therefore the need for the market to self-regulate. The other camp of scholars treats privacy as a right given that access and usage of data is beyond the user's knowledge. It activates the role of the state in providing protection through legislative frameworks.

Treating privacy as a right, almost all participants alluded to the role of jurisdiction and judicial courts to prevent the Jordanian government's illegal access. However, this view only tackled the need to regulate official entities' surveillance practices. Not one participant of the eight who answered this question mentioned the need to regulate private sector use.

Since "official entities" were the main common threat that activists identified, their suggested legislations to regulate data access and sharing revolved around regulating official surveillance. Most participants believed that access to anyone's information should be granted through the judicial system rather than the security apparatus:

> I am for interception of email and privacy under one condition: the interception of terrorists who threaten society, or a country— like ISIS. I am for hacking and censoring Jihadist websites that are still accessible to protect the safety and security of the whole society. Even the interception of these websites needs a clear legislation that requires the interceptor, usually a security entity, to apply for interception permission through a specialized court. (Ali, journalist)

Those who mentioned terrorism as a possible reason for legitimate access expressed their fears about the definition's clarity and thereby the possibility of abusing the application for such access. Others were suspicious of the process through which a citizen is identified as a terrorist and believed that clear evidence rather than suspicion of terrorism makes violating someone's privacy legitimate.

> Terrorism is very loose as a definition. We can call anybody a terrorist and start surveilling him/her. Sometimes we have to [surveil] if there is a terrorist threat, but we need standards, criteria, and enough evidence to legitimize surveillance. Suspicion is not enough to violate someone's privacy. (Muna, NGO representative)

> Security forces should announce the cases in which they intercept a computer or a Facebook account. However, in reality lines are crossed, and this does not only happen in Jordan but also in the USA. After the events of September 11, many violations of privacy took place in the name of national security and fighting terrorism, and in the name of so many other things. (Ibrahim, NGO representative)

> I would definitely blame the government if some suicide bomber was able to blow himself up in the middle of the town and then they find out that they were sending out emails telling everyone and the government didn't know about it. Then I would definitely blame the government. (Ziad, activist)

All participants who gave reasons for legitimate access stated that it should be done through an "order," a "judicial request," or a "warrant."

Raya, Salem, and Batoul said that there is no legitimate reason for accessing

information in the first place, and under no circumstance is it justifiable. One lawyer suggested that warrants should be issued from a civil rather than a security entity:

> Why should the Technical Support Department be under the Criminal Investigation Unit or the Public Security Department? Why cannot this Technical Support Department exist under the General Prosecutor, and whoever works in it comes from a civil background rather than a security mentality…? If a personal data department or committee is to be established, it should not involve the Minister of the Interior but the Minister of Justice. If there was a need to intercept someone's data or information, the decision should be made through a justice department and not the Criminal Investigation Unit that is connected to the Ministry of the Interior… [It should be] a clear judicial court order that provides justification, for a specific period of time, meaning a limited period for interception. Meaning, I should review a drug dealer's phone calls from the beginning of the year, not from the day he was born. (Rula, lawyer).

VIII. Conclusion:

- **Despite actors' suspicions about the security of communication media, the Internet is considered a vital tool for human rights endeavours.**

  What is private for most human rights actors who participated in this research is not their work-related activities or oppositional opinions but information about their family and friends. Their endeavour is to communicate their messages and activities around human rights issues in Jordan, but they are afraid to be blackmailed by getting their families or friends hurt as a result of their activities. The Internet for human rights actors still serves as platform for mobilization, activism, public awareness, and outreach to victims. However, their main concern involved exposing their sources who request anonymity.

- **Human rights actors' perceptions of possible private digital zones are highly dependent on the larger political context in Jordan, their individualized experiences and technical awareness.**

  Activists, lawyers, and NGO workers' perception of possible private digital zones in Jordan were influenced by one common factor: the reality of the corresponding political context in Jordan. Participants' awareness of the tight institutional and legislative environment to practice freedoms, and the lack of transparency and law enforcement, made them question the possibility of absolutely private digital zones. While such absolute private zones did not exist for participants, imagining "safer" spaces was influenced by highly individualistic and contextual experiences.

  What constitutes a private zone for participants depended on many variables: the perceived sensitivity of one's online activities, perceptions of third-entity access to information, perceptions of data availability, first-hand experiences, and the "trust factor" in private companies and platforms. However, the most decisive factor in perceiving the possibility of a "safe zone" involves answering "safe from whom?" Most participants believed that safe zones could not exist if personal data or communications were targeted by official entities. When it comes to preventing other online groups' access, there were those who believed in controlling the reach of posts they share on social media through privacy controls offered by these spaces. Others believe that some platforms are "safer" than others based on either first-hand hacking experiences or news they read about the different companies' collaboration with intelligence agencies.

  When it comes to users' knowledge of available personal information online, visibility, for all participants, meant availability. The information they perceived was available included all visible posts, pictures, published work, and so on. However, none of the participants mentioned non-visible data such as meta-data or their navigation history, for example. The limited technical knowledge of online trails formed their perceptions of what should be protected.

- **Official entities and intelligence agencies were the most commonly perceived third parties with access to participants' private data and communications.**

  While companies and different online groups were mentioned as third entities who might have access to their information, it was not as concerning to participants as official entities' access. Most participants listed the Intelligence Department as the entity most likely to threaten access to their private communications because their political online voices spread between public and private platforms. Private

companies were the second most commonly perceived entities with access to personal and private data, however, this access was deemed less threatening than Intelligence Department access for participants.

- **Perceptions of surveillance do not translate into the adoption of security tools. Self-censorship and conscious selection of communication tools are the most prevalent actions by which users attempt to protect their privacy online.**

  Very few users used high-tech security tools like encryption and TOR (an anonymity browser). Fewer people believe in the possibility of digital private zones than those who gave up on controlling information online. The more politically active the participants were, the less personal information they shared on social media platforms. Most participants who said that they started limiting their personal content online referred to content related to family because they did not want to put their families at a risk as a result of their work activities. When it comes to protecting the information of others, journalists and NGO workers used more drastic measures. They either changed their communication behaviour through choosing a face-to-face interaction when handling sensitive information, or concealed or erased any traces of their sources' names on their devices.

- **Regulating digital privacy means regulating "surveillance."**

  Participants' views on suitable legislations to regulate access to personal information consolidated with their perceptions of entities that they found most violating. Participant suggestions for a regulatory framework did not go further than the regulation of surveillance by official entities, especially in the name of terrorism. There was no mention of the need to regulate commercial entities' use of their data through a solid data protection law.

This research's findings should be understood within the context of its timing in 2014. This research was conducted at a time when human rights activism faced a general setback in the rise of a post-2011 revolution's chaos and insecurity across the region. This setback slowed down social mobilization to achieve democratic reforms in governing executive, legislative, and judicial institutions. Therefore, the consciousness of human rights actors around digital private zones, and the security of their communications and data, are highly influenced by the direct threat that they perceive. For participants, the direct threat in the research period was the official entities' access that most people thought was inevitable. This led participants to restrict sharing information about their family and friends on social media websites as the main method of protection. Protection from hackers and other online monitoring groups was done through activating complex passwords and privacy features on social media. However, most did not perceive their oppositional political opinions as information to be protected because public communication is a main factor in their human rights endeavours.

The question of what should be private and how private in our communication remains to be answered. In a state like Jordan that is heightening its policies and procedures to keep it safe from alleged threats of instability, access to official information becomes more and more difficult. This research is a first step in documenting the importance of privacy as a right among active human rights actors, and documenting first-hand stories on data access and protection from

several entities. We hope that this research will inform the global discourse on the importance of context when it comes to the debate on the right to privacy and assumptions about activists' adoption of security tools. This research will serve as a base for further comprehensive research and documentation on data access and sharing practices across private sector and public institutions in Jordan. Finally, we hope that this research will be a reference for policy-makers and private companies to inform the laws on data protection and advocates who defend the "right to privacy."

Appendix I: **Interview Questions**

1. Introduce yourself. What is the nature of your work and activities?
2. Describe your relationship with the internet (to which extent do you use it in your work? what applications and websites do you mainly use?)
3. Do you use the Internet on your phone? (what applications and websites do you mainly use?)
4. In your opinion, what kind of information is available on you online?
    a. What information do you volunteer to share?
    b. Are any of it information that you did not volunteerr to share?
5. In your opinion, are there any third parties accessing/using available information about you online or information stored on your mobile phone?
    a. If yes, what kind of third-parties (companies, official entities, employers, family)?
    b. What kind of information do these third parties use?
    c. How is this information being used?
    d. How did you formulate your perceptions about third parties access and use of this information?
6. Prioritize this info according to what should be protected the most?
7. In your opinion, are there safer spaces/methods to communicate than others?
8. Who, in your opinion, are most likely to be a subject of interception?
9. Do you follow any practices to protect your information online or on your mobile phone? What are they?
10. Is there any legitimate reasons for a third-party to access your personal info?
11. What, in your opinion, should the legislative framework to protect access to your information look like?

Appendix II First- and Second Second-Hand Stories:

First-hand Stories

Laila the journalist experienced listening to her own recorded conversation:

> Something happened to someone right in front of me. He is from the political opposition. We were talking about something non-political. Ten minutes later, his mobile phone rang and we heard the entire conversation recorded back. After that I cut all my ties with politics because I was truly scared. (Laila, journalist)

Raya the activist planned a fake demonstration to test if her phone was being monitored:

> We tested them [intelligence forces] several times. We would announce false demonstrations—in a phone call or text message—in front of the royal court, for example, and then we'd go and find them there. They were not real demonstrations, but we would do that to see if they would find out. (Raya, activist)

Ibrahim experienced finding security apparatus waiting in a public event that he announced on Facebook:

> When we posted a Facebook event announcing a youth debate, we found three police cars waiting for us, before even the arrival of the banners or volunteers. All of our activities are attended by security apparatus. In the war against Gaza in 2012, we were organizing a small event for people to write supporting statements in solidarity with Gaza. We were surprised to find 300 members of the gendarme, well prepared… the people we invited got scared and left ... We had invited fifty to sixty people through Facebook—it was a public event. (Ibrahim, NGO representative)

The journalist Muhanad has never been personally intercepted but he confirmed that an intelligence officer is assigned to each media organization and said that this was "common knowledge." However he experienced a story involving his employer and the ISP:

> When a colleague of ours had issues with the management, he exchanged a couple of emails through which I advised him on his rights. I later found out that our ISP provided the management with access to all my emails, through which the management was able to accuse me of inciting my colleague against the company. (Muhanad, journalist)

Rula, the lawyer who defends political prisoners, mentioned getting calls from private numbers confirming that they know intimate details about her personal life and threatening her that they would send pictures to her husband abroad. She also had experiences with her email account:

> There was a year where my Hotmail account was closed—I created one on Yahoo and that was shut down too. I created another one on Yahoo and it shut down. I felt I was under surveillance—how did they find my new email? How did they access it? (Rula, Lawyer)

Ziad said that he formed his perceptions from his followers on Facebook and Twitter:

> From the likes I get on the page and Twitter some of them are clearly

> not active users. Some of the likes I get from profiles that are obviously not being used for personal reasons. And on Twitter you get someone who follows you and has no followers and no tweets and is following like 200 people. When a friend of mine was coming back from Belgium, they stopped him at the airport for three or four hours; they interrogated him. Just a general interrogation: why did you post this stuff on Facebook? And so on. (Ziad, activist)

Second-hand Stories

Lama mentioned attempts to discredit a Jordanian political activist who was held in Saudi Arabia:

> The biggest example on Twitter is Khalid Natour. When Khalid was imprisoned in Saudi, people who were against the movement started uploading screenshots of things he used to post in the past, to discredit him and weaken his position … There was also the story of the Raba'a youth who were taken to court based on private WhatsApp messages. (Muna, activist.)

Others like Amar mentioned the news about the case of charging three citizens with "harming relationships with a foreign country" for distributing the symbolic sign of the Muslim Brotherhood in Egypt. One of them was charged over a WhatsApp message:

> No, I've never experienced anything directly no … There was the case last fall where a guy was arrested, one of the "Hiraki" activists. Three were arrested on the charge of harming Jordan's relations with a foreign state, and the state security court at the time. Anyway one of the three apparently was additionally charged with "Italet Al Lisan" which is insulting the king based on WhatsApp messages. So that could be a situation where he was arrested and they got his phone and they got him to give them the password so they can see it, but it could also be that they were somehow reading his WhatsApp messages. (Amar, NGO representative)

Salem questioned whether cases of surveillance were real or just an attempt to create an impression that they were:

> We used to joke and say everything is under surveillance, but we later realized that it is true. This happens in a country the size of America, so what do you expect in Jordan? … But again this has to do with them creating the impression that you are under surveillance. (Salem, journalist)

The research team could not validate these stories. Validating these stories with evidence beyond the high credibility that respondents have socially tis not possible. Even though first-hand stories where not triangulated, together, they make a step forward into the documentation of illegal access to personal information and remain highly relevant to this research.