HEINRICH BÖLL STIFTUNG
MIDDLE EAST

# Fighting against “Nothing to hide”

–

## Civil Society’s Experiences of Advocating for data protection in Lebanon

Katharina Schmidt

September 2018

# Outline

Introduction ..... 2
Methodology ..... 3
Data protection in Lebanon and rationale to study ..... 4
Reasons for the lack of Public debate about data protection in Lebanon ..... 5
Historical factors: No "historic shock" ..... 5
"No priority": Hierarchization of rights ..... 6
Socio-cultural factors: Lack of appreciation versus lack of knowledge ..... 7
Data protection as a double-edged sword? ..... 8
Survey Findings: Public opinion about privacy and surveillance ..... 9
Value and state of privacy protection ..... 9
Knowledge ..... 9
Attitudes towards surveillance technologies ..... 10
Prioritization ..... 10
Discussion and Conclusion ..... 11
List of Civil Society Actors interviewed ..... 13
References ..... 13

# INTRODUCTION

> *"I once attended a training of an insurance company on the topic of how to best attract new customers. The trainer suggested we should make use of our personal network – ideally asking medical staff if they can't provide access to some of their large patients' databases. I was shocked, this practice goes against so many norms and laws regarding privacy rights! When I protested, the trainer only replied that if I don't feel comfortable doing this, I should just not do it. But no, I mean, that's not how it should be! We should have a discussion about this!"*[1]

The question of how personal data should, and more importantly, should not be used has increasingly gained traction over the last years.[2] While surely not a new phenomenon, the possibilities to collect, store and process personal data by state as well as private actors has heavily increased due to technological advancement – and with it the concerns these new developments entail for the freedom and safety of people. As has been pointed long ago, access to large data-sets of personal information constitutes a prerequisite for social control, allowing those who hold such data to influence the behaviour of those whose data is being held (Stadler 2002, Solove 2008). Today, misuses of personal data range from private companies tailoring their marketing campaigns or trading personal data with third parties to states' security agenda under the proclaimed need for enhanced surveillance through "bulk interception" of citizen's data.[3] While these developments have put the topic of data protection on the public agenda in many countries, it remains "marginalized" in Lebanon as one respondent interviewed for this paper framed it. While much has been written about the way advocacy groups in the US and Europe have criticised such practices as violations of citizen's privacy rights (Dencik et al. 2016, Löblich/Wendelin 2012), much less scholarship focuses on responses to dataveillance in non-Western contexts (Dencik et al 2017). As has been stated, civil society's advocacy for improved privacy rights in the digital age has been influential in legislative changes strengthening individual privacy, with many countries adapting their privacy framework to new digital conditions.[4] The most recent and encompassing example is the European Union's (EU) General Data Protection Regulation (GDPR) that went into force in Mai 2018, seen as the world's most encompassing data protection legislations to date (Dencik et al 2016, Times 2018).[5]

---

[1] Personal anecdote of one of the respondents
[2] Personal data is here defined as every information allowing the identification of an individual person (examples are name, home or email address, physical location etc.)
[3] This practice has been termed "dataveillance" (Haggerty and Ericson 2006).
[4] Privacy International lists 126 countries as having adopted privacy regulations regarding personal data https://medium.com/@privacyint/data-protection-across-the-world-fe66ca1e138f
[5] Available at https://eur-lex.europa.eu/eli/dir/2016/680/oj

Meanwhile – being a conflict- and terrorism-affected country in a fragile region – Lebanese security and government actors are deploying surveillance and data collection technologies that outpace the development of adequate legal protections for their citizens' data (Privacy International 2018). In effect, Lebanon, with very little legislation regarding privacy rights to begin with, has not yet introduced legislation regarding the protection of personal data (ibid.). This motivated this research into the reasons civil society actors identify for its relative negligence. Specifically, this research is guided by the following questions:

- From the perspective of civil society actors in Lebanon, what are the reasons for a lack of data protection legislation in Lebanon and what barriers do they face in putting the issue of data protection and privacy rights on the public agenda?
- What is the general public opinion and awareness regarding data protection and privacy rights?

After outlining my methodology, I will give a short overview about the legislative framework regarding data protection and privacy rights in Lebanon. I will then go on discussing what civil society actors perceived as the main reasons for a lack of data protection and barriers of increased advocacy. I will present findings of a small-scale survey among young academics' opinion regarding privacy, and discuss findings from both research strands.[6]

## METHODOLOGY

The study is based on desk research of NGO reports and journalistic reporting as well as seven semi-structured interviews with directors of advocacy organizations, researchers and activists who engage with the topic of data protection in their work (a full list of respondents can be found in the annex). They were chosen on the basis of their interaction with the subject, such identified in their online presence or as being quoted as experts in media coverage. The face-to-face interviews were conducted in Beirut between July and September 2018 and lasted between 25 and 60 minutes, one interview was conducted on the phone. Among the civil society groups interviewed were two that explicitly focus on the issue of digital rights, namely the organizations Social Media Exchange (SMEX) as well as the Samir Kassir Eyes (SKeyes) Center for Media and Cultural Freedom and two that feature a more general human rights agenda, namely Lebanon's branch of the international organization Human Rights Watch, and the Lebanese organization Legal Agenda.

[6] For the purpose of this research, civil society actors are defined as individuals and organizations from the non-governmental and non-commercial sector (Hintz and Milan 2009: 23) engaged in "mobilised networks of groups and organizations, who over a certain period of time try to induce, prevent or undo' certain regulations and who apply political strategies in order to become integrated into the political process" (Kern, 2008: 13).

In addition, for the purpose of data triangulation and additional descriptive analysis, a small-scale survey has been conducted in addition to the qualitative interviews. The survey was based on existing research about public opinion about privacy, surveillance and data protection in other countries (see Budak et al 2013), slightly adapted to include points mentioned in the first interviews. The 27 questions covered opinions about the value of privacy in general and the perceived state of privacy and data protection in Lebanon as well as attitudes towards surveillance. In addition, it assesses to what extent respondents are in favour of the "nothing to hide argument", the very powerful, though false, justification for surveillance intrusion of people's privacy.[7] Due to the exploratory nature of this research and the small scope of this research, it was decided to limit the target group to a sample students and graduates between 20 and 35 years, with a sample of 30 respondents. The survey was distributed online with the help of personal contacts and social media channels of hbs and SMEX as well as in printed form at the American University of Beirut in the months of August and September 2018. [8]

## DATA PROTECTION IN LEBANON AND RATIONALE TO STUDY

Internationally, data protection legislations have evolved as an expansion of legislation protecting citizens' privacy in the digital age (Tzanou 2013). While the Lebanese Constitution states in its preamble that Lebanon as "a founding and active member of the United Nations Organization" abides by the Universal Declaration of Human Rights, including the human right to privacy, the constitution itself does not explicitly protect privacy.[9] Lebanese law contains articles protecting the inviolability of the home (Article 14), as well as individual liberty and freedom of expression (Articles 8 and 13). As such the legal framework protecting citizens' privacy is weak (ibid.). Similarly, even though Lebanon is part of international directives on data protection, such as the one issued by the United Nations Economic and Social Commission for Western Asia (ESCWA) in 2012, the country lacks specific and comprehensive legislation on personal data, only protecting data privacy in specific sectors (for an in-depth discussion of the legal framework see SMEX 2015/2018).

Despite this weak legislative framework, the Lebanese government has heavily increased its surveillance capabilities and data collection tools, such as introducing large scale surveillance camera coverage in 2016 in Beirut, without legal oversight and little public discussion (SMEX 2016). In addition, Lebanon began issuing biometric passports and residency permits in 2015,

[7] For an in-depth discussion of this argument see Solove 2007
[8] This choice was also influenced by my favorable access to this group due to existing contacts and the need to conduct the survey in English due to my inproficiency in Arabic.
[9] Lebanese Constitution, available at http://www.wipo.int/edocs/lexdocs/laws/en/lb/lb018en.pdf

thereby expanding the amount of data it now collects from its residents without clarifying how it is protected (ibid.). Cases of spy software usage by government actors have been reported over the years, pointing towards systematic surveillance of Lebanese citizens (Human Rights Watch 2018).[10] One of the most recent data breaches include the publishing of Lebanese expat voters' personal data during the 2018 election.[11] In addition, as an example how state and corporate data gathering and surveillance practices are interlinked in Lebanon, SMEX reported how the two state-owned mobile phone operators Alfa and touch sell their customers' data to advertising companies, resulting in spam messages SIM card owners receive regularly (SMEX 2018). That suspects are regularly persecuted on basis of their private data or private communication in front of courts and the way the current crackdown on activists is amplified by a non-protection of personal communication and data protection were other main concerns raised by the respondents interviewed. However, the majority of the respondents believed the topic is absent from public debate in Lebanon, or, if present, quickly gets overshadowed by other issues.[12]
In the following I therefore present reasons identified by the respondents for this lack of public debate around data protection in Lebanon.

## REASONS FOR THE LACK OF PUBLIC DEBATE ABOUT DATA PROTECTION IN LEBANON

### HISTORICAL FACTORS: NO "HISTORIC SHOCK"

One reason for the lack of data protection in Lebanon is seen in the lack of what one respondent called a "historic shock": In Lebanon "people are not coming to privacy from a struggle like Germany for example", says Mohammad Najem, founder of Beirut based NGO Social Media Exchange (SMEX) in reference to the systematic abuse of private data by the Nazi regime to identify Jews and other minority groups, as well as the human rights violations during the surveillance state of the Stasi regime in East Germany.[13] This shocking example "of what people can do with the collection of data" has not only created a public sensitivity concerning massive data collection and the basis on which society can get mobilized (ibid.). "But here, we are not coming from anywhere where the collection of data has been a problem" (ibid.), in contrast, according to Najem, the use of data has always been perceived as a simple way to make life easier

[10] see http://www.dailystar.com.lb/News/Lebanon-News/2018/Feb-06/437019-dark-caracal-lebanon-in-the-age-of-cyberwarfare.ashx, https://www.eff.org/deeplinks/2015/08/hacking-team-leaks-confirm-what-arab-privacy-advocates-already-knew
[11] https://smex.org/lebanese-embassies-expose-the-personal-data-of-registered-voters-living-abroad/
[12] See also http://www.beirutreport.com/2015/07/whos-got-your-data-2.html
[13] The formulation of the right to privacy in the General Declaration of Human Rights as well as the privacy protection legislation developed in Europe are heavily influenced by the experiences of World War II (Time 2018).

– with mobile applications heralded as solutions for daily difficulties, and adopted with little or no interrogation of the privacy risks included.

In addition, while the revelations by Edward Snowden in June 2013 are seen to have significantly influenced the shaping of the GDPR, transforming it from a "boring topic" without public attention to a story about US spying on EU states, allowing civil society to capitalize on public attention in their demands for stronger regulation (Kalyanpur/Newmann 2018), its focus on Western states has limited its impact on public opinion in Lebanon, says Najem.[14] While "Snowden definitely helped" in raising awareness on the issue of data protection, it has not received as much attention in Lebanon as in Western countries (ibid.). In contrast, according to some respondents, this year's scandal around Facebook users' data being intercepted and used by private companies for targeted election campaigning in the US and several other countries has been more influential. The video of Mark Zuckerberg being questioned in front of the US court around data practices by the company was widely shared among Lebanese, and "triggered" Lebanese to perceive data protection as a serious concern, eliciting some of the scarce mainstream media coverage on this issue.[15]

## "NO PRIORITY": HIERARCHIZATION OF RIGHTS

There is an agreement among the respondents that data protection is not perceived as a priority for policy makers or the public alike. In light of other problems in Lebanon conceived as more serious such as the bad economic situation, the general perception is that "people sacrifice" their right to data privacy, as Najem frames it, or simply have "other priorities", says Nizar Saghieh, Deputy Director of Legal Agenda. Ayman Mhanna, the Executive Director of SKeyes Center for Media and Cultural Freedom experiences that data protection is perceived "as a luxury", detached from issues such as economic impoverishment.

This prioritization was also found among the civil society groups featuring a more general human rights agenda. As Lama Fakih, Deputy Middle East Director of Human Rights Watch, put it: "If you'd ask me to initiate a project on data protection for the next year, I would say no. There are far more extensive and egregious rights violations that we need to tackle, from environment, access to education, or access to work. It's not priority one, but it's an important issue". According to Saghieh, the quest for data protection, as a "very sophisticated privacy issue" is a few steps ahead in a context where not even privacy is secured by law: "Before you start talking about the protection of personal data you must ensure privacy" with data protection seen as "one of the effects of the right to privacy". Referring to the example of the criminalization

[14] Snowden documented large scale state-corporate data collection of communication networks in Western democracies, mainly by the NSA and the British Government (see Kalyanpur/Newmann 2018)

[15] http://www.dailystar.com.lb/News/Lebanon-News/2018/Apr-16/445387-facebook-scandal-raises-questions-over-data-protection.ashx

of homosexuality, he states that as long as the Lebanese state is criminalizing private issues, requesting measures for data protection presents a severe challenge (ibid.).

This argument, that personal privacy has to be traded against collective security – probably the oldest barriers in anti-surveillance struggles all over the world – is believed to remain "very powerful" in the public's discourse, says Mhanna, and tends to favour security over privacy rights. These are, in the words of Fakih, "seen as more debatable in light of terrorist groups that are organizing on facebook", observing that there is "a willingness to sacrifice privacy in order to keep safe". Similarly, Joseph Helou, Political Scientist and Social Movement Researcher at the Lebanese American University, argues that "It is easy to talk about protection of personal data when you are in the US or Europe, but not so when you are in the Middle East, with ISIS just next door and where you have all these ominous threats that may pose security explosions at any point in time".

## SOCIO-CULTURAL FACTORS: LACK OF APPRECIATION VERSUS LACK OF KNOWLEDGE

Legal scholars have argued that the right to privacy is based upon premises of individualism, as "essentially the right not to participate in the collective life — the right to shut out the community" (Thomas Emerson, cited in Tzanou 2013). This common interpretation of privacy rights is shared by many of the respondents. As Saghieh argued: "Privacy rights are part of societies based on individualism", whereas in Lebanon communitarian and sectarian concerns are valued more than individual issues. "There is very few space for individualism in Lebanon" with possible consequences of how people deal with their information. "When you are living in a community you don't talk about protecting data, you talk about sharing data". The view, that the communitarian value inherent in the Lebanese society inhibits appreciation for the right to privacy is also shared by other respondents. Adriana Basbous, who uses creative art work for activism against surveillance and recently designed a project in collaboration with SMEX for this year's Beirut Design Week, argued that "there is a strong will in the Lebanese society to have a community, to have strong ties with your family, where personal privacy is not seen as necessary. I believe this affects the way we look at the issue of data protection, it is less seen as an issue".
The question in how far cultural values influence the negligence of data protection was however contested: As Mhanna argued, that while acknowledging that privacy might be socially differently conceived in Lebanon than in other countries, people's practices are better explained by a lack of knowledge of what happens to this data than a non-appreciation of personal privacy:

> "I don't think we've reached a point where people are thinking about what they would like to keep private and what they would like to expose. For example, we are a society that is on many items extremely conservative, yet we have no problem in

> putting information that we would like to hide from our neighbours, we put it online, not understanding how it works."

This is also reflected in the assertion of Joulia Bou Karroum, freelance consultant for Lebanese NGOs who formerly worked for Amnesty International, arguing that social media platforms are seen as "safe spaces", pointing to the lack of digital knowledge especially among older generations. Communitarian values then turn into social pressure to share personal data online, especially in light of the Lebanese great diaspora and the desire of family members abroad to stay up to date, for which communication technology provides the means. Karroum illustrates this with the example of young mothers creating social media profiles of their offspring, and the common practice of posting and sharing photos of their children online – and the criticism especially women face from family members when refusing such online exposure of their families. All the respondents argued that the little awareness and claim for data protection is due to a lack of knowledge what happens to citizens' personal data and why protecting it is important.

## DATA PROTECTION AS A DOUBLE-EDGED SWORD?

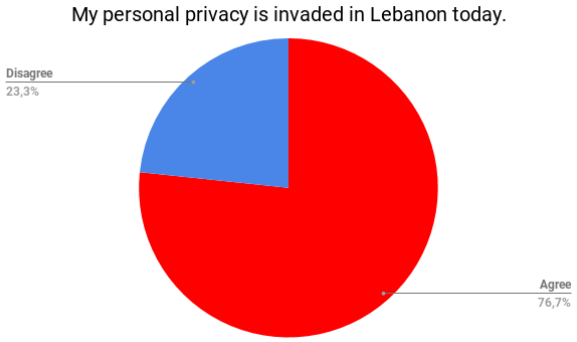
Lastly, as one respondent argued, in a context were government accountability and transparency is absent and corruption widespread, increased data protection can also present a double edged sword: According to Saghieh, the value of private data can be misused and become "dangerous in the fight of corruption", when used by governments in order to conceal public information. When asking government institutions for more access to documentation and information based on the new law on access to information, the organization experienced that the argument of protection of private data is used in order to hide government data from the public, especially when it relates to contracts with private companies. "As long as there is no clear definition of private data, state actors try to enlarge its definition in order to fit their own interests", says Saghieh. Referring to current developments in Tunisia, where the government tries to include companies' data in a draft law on data protection, the respondent argued how a push for data protection by civil society can be twisted: "Now it is even more used by the government than by activists because they don't want to give access to documents", says Saghieh.[16] While this calls for clear definitions of personal data in contrast to government and private sector data in any attempts to push for better data protection, it also highlights dilemmas and barriers of increased advocacy on data protection in Lebanon: "What is the priority? Is it more transparency or more protection of private data? If you are living in a country where there is no accountability at all of course your priority is more transparency", says Saghieh.

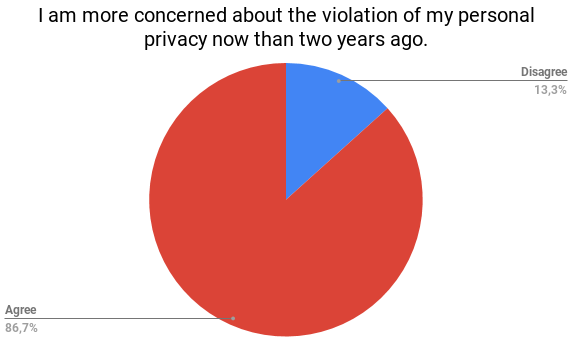
[16] https://www.article19.org/resources/tunisia-wpfd-government-rolls-back-freedom-expression-gains-tunisian-revolution/

# SURVEY FINDINGS: PUBLIC OPINION ABOUT PRIVACY AND SURVEILLANCE

## VALUE AND STATE OF PRIVACY PROTECTION

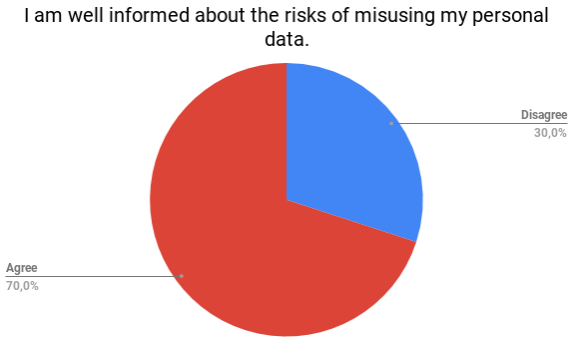
All of the respondents stated that the protection of personal privacy is of great importance them, while above 75% agreed to the statement "My privacy is invaded in Lebanon today". In addition, all stated to be more concerned about personal privacy violations than two years ago. A large majority believed the current legislation does not protect personal data enough (87%) and believes that Lebanon needs better legislation for data protection (97%).

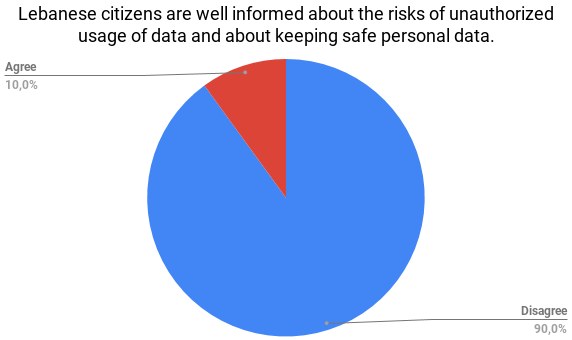



## KNOWLEDGE

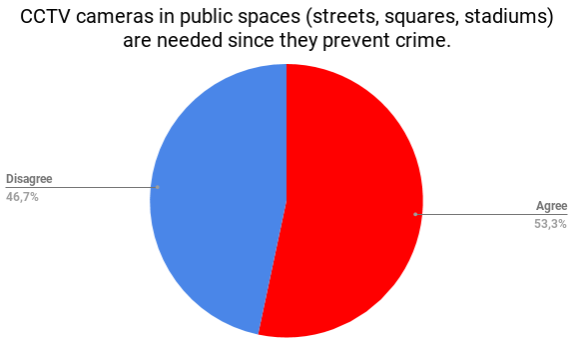
While around two third stated to be well informed about the risks of misuse of their personal data, only 10% believed that Lebanese in general are well informed about risks of unauthorized usage of personal data. Almost all (93%) of the respondents therefore agreed with the statement that there should be an increased education about the risks of lacking data protection.

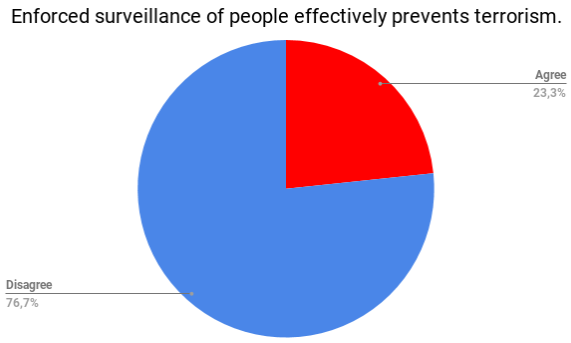


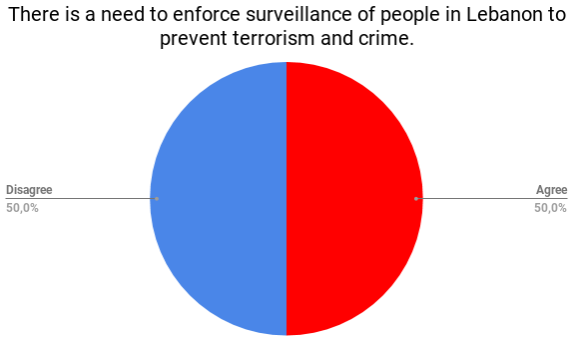



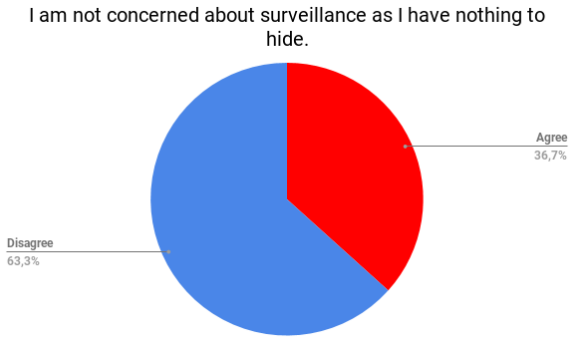
## ATTITUDES TOWARDS SURVEILLANCE TECHNOLOGIES

Attitudes towards surveillance were more mixed, with a small majority believing surveillance cameras as being needed to prevent crime, while being less in favour of the statement that surveillance prevents terrorism. Interestingly, still half of the respondents saw a need to enforce surveillance in order to prevent terrorism and crime. Either way, the majority (73%) found that security agents should not have unrestricted access to citizens' data in order to prevent crime. Still, one third of the respondents was in favour of the "nothing to hide" argument.



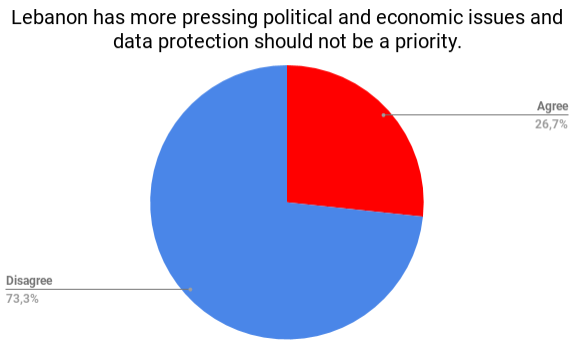



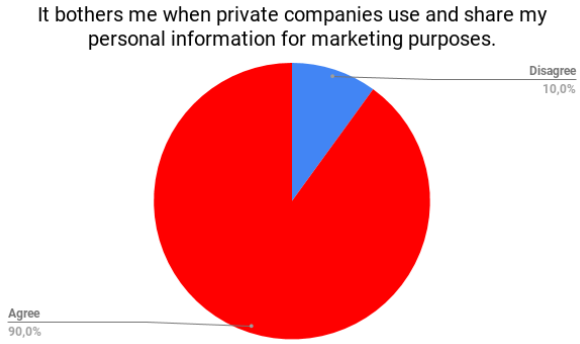




## PRIORITIZATION

Only one fourth believed that Lebanon has more pressing political and economic issues and data protection should not be a priority. Equally, the willingness to sacrifice ownership of data against economic benefits was low: 90% stated they are bothered when private companies trade their data for marketing purposes and only one third stated to not mind exchanging personal data for free services.




## DISCUSSION AND CONCLUSION

I have tried to flesh some of the problems that civil society actors encounter in raising awareness on the issue of data protection in Lebanon encounter, revolving very much around the question of why it is not perceived as an important topic by the general public. The reasons given address historical experiences, the lack of legal protection of privacy as a foundation to data protection, prioritisation of rights and needs as well as a lack of general knowledge. Socio-cultural factors have been noted as important as well, while their role remained contested. The survey found a high value attributed to the protection of personal privacy and concern about privacy invasions in Lebanon as well as the voiced need for improved legal protection. In line with the observations about the impact of recent international data scandals, survey respondents stated an increased concern about data protection compared to two years ago. They saw themselves as better informed about risks of misuses of personal than the general public, whose knowledge was rated as very low, agreeing on a need for increased education on this issue. These findings most probably reflect the specific demographic sample chosen here, as highly educated are generally more knowledgeable and cautious in relation to data protection (Budak et al 2013) but also contributes to the argument that it is more an issue of lack of knowledge than appreciation of privacy that explains observed relative negligence of the topic. While the concern about misuses of own personal data were high, attitudes towards surveillance were more favourable, with half of the sample being in favour of increased surveillance in order to prevent crime and terrorism. This reflects the rationale of the nothing to hide argument, explicitly supported by one third of the respondents. It can be hypothesized that these findings are specific to the special

demographic and call for a comparison with other demographics, also taking class, ethnic and sectarian background into account in order to understand how attitudes and priorities differ. [17]

In addition, two barriers to an increased advocacy on the topic of data protection among civil society actors emerged: One is the prioritisation of rights ascribed to public attitudes that has also been found among the advocacy groups that engage in more general human rights activism – arguing that there are still more important rights abuses to tackle. The other points to the struggle of pushing for increased data protection in a context struggling for increased transparency and accountability. These findings point to the limitations of the discourse on privacy rights when advocating for data protection. While not downsizing its value as a crucial human right, the concept of privacy is in itself so fuzzy and subjective that it came under scrutiny in its ability to mobilize for the cause of data protection (Stadler 2002). This ability, above findings suggest, is even further reduced in a context where legal framework regarding privacy is weak and social norms ambiguous. Recently, scholars have suggested to expand advocacy on data protection as a social justice issue (Dencik et al 2016), thereby including not only privacy violations but also the way disrespect for data protection leads to economic exploitation, discrimination and social sorting in an increasingly data-driven world (ibid.). Framing the necessity to protect personal data not only as a matter of privacy rights, but as a matter of "data justice", might help to emphasize the consequences of misuses of large amounts of personal data in their capacity to exploit and discriminate against social groups (see Lyon 2014, Bernal 2016). This might help to advance the right to personal data protection as an own right next to the right to privacy, not simply as a consequence of the latter (Tzanou 2013) and help transcend the current trade-off between economic justice and privacy rights highlighted by the respondents. As formulated by Mhanna:

> "People take it as a luxury, now we have economic problems, let's not talk about that. Well, you might have worse economic problems soon, your jobs are replaced by software and robots, and we are not talking here about non-qualified jobs, we are talking about AI replacing lawyers. Well yes, you didn't pay attention when it matters, so let's start to pay attention now."

[17] Research on has shown how these are important indicators for perceptions of security in Beirut, possibly paralleling attitudes towards surveillance as well (Fawaz et al 2012)

## LIST OF CIVIL SOCIETY ACTORS INTERVIEWED

(#1) Mohammad Najem, Founder of Beirut based NGO Social Media Exchange (SMEX), 27.07.2018
(#2) Joseph P. Helou, Political Scientist and Social Movement Researcher at Lebanese American University, 02.07.2018
(#3) Adriana Basbous, engineer and scientist who uses creative work for activism against surveillance, designed a project in collaboration with SMEX for Beirut Design Week 2018, 03.08.2018
(#4) Lama Fakih, Deputy Middle East Director of Human Rights Watch, 31.08.2018
(#5) Ayman Mhanna, Executive Director Samir Kassir Eyes (SKeyes) Center for Media and Cultural Freedom, 04.09.2018
(#6) Joulia Bou Karroum, freelance consultant for Lebanese NGOs, former Middle East Branch of Amnesty International, 06.09.2018
(#7) Nizar Saghieh, lawyer and Deputy Director of the Lebanese NGO Legal Agenda, 06.09.2018

## REFERENCES

Bernal, Paul (2016): "Data gathering, surveillance and human rights: recasting the debate". Journal of Cyber Policy, 1:2, 243-264,

Black, E. (2002) *IBM and the Holocaust: The Strategic Alliance between Nazi Germany and America's Most Powerful Corporation*. New York: Three Rivers Press, Random House.

Budak, Jelena , Ivan-Damir Anić & Edo Rajh (2013) Public attitudes towards privacy and surveillance in Croatia, Innovation: The European Journal of Social Science Research, 26:1-2, 100-118,

Couldry, Nick; Ulises A. Mejias (2018): Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject. *Television & New Media*: 1–14

Dencik, Lina; Arne Hintz and Jonathan Cable (2016): Towards data justice? The ambiguity of anti-surveillance resistance in political activism. Big Data & Society July–December 2016: 1–12

Electronic Frontier Foundation (EFF) (2012): Data Request from Lebanese Security Agency Sparks Controversy. https://www.eff.org/deeplinks/2012/12/lebanese-security-agency-user-data-request-sparks-controversy

Fawaz, Mona; Mona Harb; Ahman Gharbieh (2012): "Living Beirut's Security Zones: An Investigation of the Modalities and Practice of Urban Security". City & Society, Vol. 24, Issue 2, pp. 173–195,

Ginsburg, Jodie (2018): "The data protection bill poses a real threat to the media's ability to hold the corrupt to account". The Independent https://www.independent.co.uk/voices/data-protection-bill-media-freedom-press-index-censorship-rupert-murdoch-paul-dacre-a8339786.html

Gunther, A., Perloff, R. & Tsfati, Y. (2008). Public opinion and the third-person effect. In W. Donsbach & M. W. Traugott *The sage handbook of public opinion research* (pp. 184-191). London: SAGE Publications Ltd doi: 10.4135/9781848607910.n18

Haggerty, K. D., and R. V. Ericson, eds. 2006. The New Politics of Surveillance and Visibility. Toronto: University of Toronto Press.

Hintz A and Milan S (2009) At the margins of internet governance: Grassroots tech groups and communication policy. International Journal of Media & Cultural Politics 5: 23–38.

Human Rights Watch (2018): "Lebanon: Investigate Large-Scale Surveillance Reports". https://www.hrw.org/news/2018/01/24/lebanon-investigate-large-scale-surveillance-reports accessed 15.09.2018

Kalyanpur, Nikhil ; Newman, Abraham (2018): "Today, a new E.U. law transforms privacy rights for everyone. Without Edward Snowden, it might never have happened". Washington Post https://www.washingtonpost.com/news/monkey-cage/wp/2018/05/25/today-a-new-eu-law-transforms-privacy-rights-for-everyone-without-edward-snowden-it-might-never-have-happened/?utm_term=.02d7ccde47e1 accessed 12.09.2019

Kern T (2008) Soziale Bewegungen: Ursachen, Wirkungen, Mechanismen. Wiesbaden: VS Verlag.

Milan, Stefania; Trere, Emiliano (2017): "Big Data from the South: The beginning of a conversation we must have". Data activism. https://data-activism.net/2017/10/bigdatasur/ accessed 15.09.2018

Löblich, Maria ; Wendelin, Manuel (2012): ICT policy activism on a national level: Ideas, resources and strategies of German civil society in governance processes. New Media & Society, September 2012, Vol.14(6), pp.899-915

Lyon, David (2014): "Surveillance, Snowden, and Big Data: Capacities, consequences, critique". ig Data & Society July–December 2014: 1–13

Privacy International: Lebanon. https://privacyinternational.org/state-privacy/1081/state-privacy-lebanon, accessed 15.09.2018

Social Media Exchange (SMEX)

- (2015): The Right to Privacy in Lebanon. Stakeholder Report Universal Periodic Review 23rd Session – Lebanon. Available at: https://www.privacyinternational.org/sites/default/files/2018-02/Lebanon_UPR_23rd_session_Joint_Stakeholder_submission_0.pdf accessed 13.09.2018

- (2016): "Mapping the Landscape of Digital Surveillance in Lebanon"
- (2017): "Building Trust: Toward a Legal Framework that Protects Personal Data in Lebanon". Available at: https://smex.org/building-trust-toward-a-legal-framework-that-protects-personal-data-in-lebanon-report/ accessed 13.09.2018

Solove, D. J. 2007. ''I've Got Nothing to Hide' and Other Misunderstandings of Privacy.'' In San Diego Law Review, 44, GWU Law School Public Law Research Paper No. 289 [online]. http://ssrn.com/abstract_0998565

Solove, D. J. 2008. ''The New Vulnerability: Data Security and Personal Information.'' In Securing Privacy in the Internet Age, edited by A. Chander, L. Gelman, and M. J. Radin, Stanford University Press; GWU Law School Public Law Research Paper no. 102 [online]. Accessed August 9, 2011. http://ssrn.com/abstract_583483

Stalder, F. 2002. ''Opinion. Privacy is not the Antidote to Surveillance.'' Surveillance & Society 1 (1): 120_124.

Stuart, Avelie; Levine, Mark (2017): "Beyond 'nothing to hide': When identity is key to privacy threat under surveillance". European Journal of Social Psychology. Volume 47 (6): 694-707

Tzanou, Maria (2013): "Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right". *International Data Privacy Law*, Volume 3, Issue 2, 1 May 2013, Pages 88–99, https://doi-org.proxy.uba.uva.nl:2443/10.1093/idpl/ipt004