Daskal, Efrat

Article

The Israeli Digital Rights Movement's campaign for privacy

Internet Policy Review

Provided in Cooperation with:
Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

Suggested Citation: Daskal, Efrat (2017) : The Israeli Digital Rights Movement's campaign for privacy, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 6, Iss. 3, pp. 1-19, https://doi.org/10.14763/2017.3.711

This Version is available at:
https://hdl.handle.net/10419/214043

INTERNET POLICY REVIEW
Journal on internet regulation

Volume 6 | Issue 3

The Israeli Digital Rights Movement's campaign for privacy

Efrat Daskal
Hebrew University of Jerusalem, Israel

Published on 19 Sep 2017 | DOI: 10.14763/2017.3.711

Abstract: This study explores the persuasion techniques used by the Israeli Digital Rights Movement in its campaign against Israel's biometric database. The research was based on analysing the movement's official publications and announcements and the journalistic discourse that surrounded their campaign within the political, judicial, and public arenas in 2009-2017. The results demonstrate how the organisation navigated three persuasion frames to achieve its goals: the unnecessity of a biometric database in democracy; the database's ineffectiveness; and governmental incompetence in securing it. I conclude by discussing how analysing civil society privacy campaigns can shed light over different regimes of privacy governance.

Keywords: Privacy, Government surveillance, Biometric

Article information

Received: 03 Apr 2017 **Reviewed:** 03 Jul 2017 **Published:** 19 Sep 2017

Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL: http://policyreview.info/articles/analysis/israeli-digital-rights-movements-campaign-privacy

Citation: Daskal, E. (2017). The Israeli Digital Rights Movement's campaign for privacy. *Internet Policy Review*, *6*(3). DOI: 10.14763/2017.3.711

Acknowledgements: *I would like to thank the participants of the Early Stage Researchers Colloquium (ESRC) of the Humboldt Institute for Internet and Society (HIIG) from 2014 and especially Ulrike Hoeppner and Jörg Pohle for their insightful ideas and advice.*

INTRODUCTION

The digital era has expanded the boundaries and meanings of basic human rights such as freedom of expression, the right to privacy, and the right to information. These changes have triggered constant deliberations between national governments, global internet corporations, inter- and nongovernmental entities over the scope of these rights (Benedek, 2008; Kay, 2014).

This paper focuses on one of these actors: civil society organisations which advocate for digital rights, also known as digital rights advocates. These organisations advocate for computer and internet-related civil liberties on parallel tracks: on the one hand, they confront governments and internet corporations in the constitutional, political, and judicial arenas, and on the other, educate the public about their rights. Thus, they are among the few social actors with the potential to challenge and sometimes even change the rules decided upon by powerful social actors (Breindl, 2011; Postigo, 2008).

In order for them to achieve their goals, digital rights advocates have to persuade other stakeholders, including the public. Yet such persuasion is not easy and usually requires them to reframe issues to their advantage. This is why, for example, the American Electronic Frontier Foundation (EFF) frames copyright issues as issues of fair use in order to legitimize expanding consumer privileges in copyrighted works (Postigo, 2008). This is also why, when dealing with net neutrality digital rights advocates worldwide have recently framed their campaigns as essential to saving the internet (Fernández Pérez, 2015; Kosoff, 2017; Panwar, 2015). Yet, only few studies explored in depth the persuasion techniques used by digital rights advocates, especially concerning the right for privacy (Bennett, 2008). This study wishes to contribute to the literature in the field by asking: "what are the persuasion techniques employed by Israel's *Digital Rights Movement* organisation (DRM) in its campaign for privacy and against the biometric database in Israel?"

To do so, I have analysed the organisation's textual products and involvement in legislation initiatives, judicial rulings, and public discourse in 2009-2017. This research sheds light on the role civil society organisations can play in constructing the boundaries of digital rights. Second, it contributes to the literature dealing with the right to privacy in a specific sociocultural context. Finally, it deepens our understanding of the global issue of privacy governance.

In what follows, I will elaborate on the role civil society organisations play in protecting digital rights, especially the right to privacy. I will then address the Israeli case, and present the research questions and methods. My findings will describe the main activities of the DRM against the biometric database, as well as the persuasion techniques employed thereby. I will conclude by discussing how the study of civil society privacy campaigns can assist in conceptualising and understanding issues of privacy governance.

CIVIL SOCIETY ORGANISATIONS AND PRIVACY: LEARNING TO SAIL AGAINST THE WIND

Governing privacy – and even the very definition of privacy – have become controversial, as new technological and socio-political forms emerge around the globe. Most studies explore privacy governance by analysing the national or international laws and regulations (Newman, 2008; Regan, 1995). Others focus on the possible influence of technological developments on privacy governance (DeNardis, 2010; Lessig, 2006). Still others examine the social interaction between different stakeholders involved in issues of privacy (Bennett 2008; Solove & Hartzog, 2014). While the latter line of analysis is still uncommon within the study of privacy governance, it coincides with contemporary trends of internet governance research, which explore the role of various social actors in internet governance processes and decisions (DeNardis & Raymond, 2013; Mueller, 2010). This paper follows this line by analysing the activities of civil society organisations in constructing privacy governance.

Civil society organisations advocating for the right to privacy differ from one another *vis-à-vis* several issues, such as their framing of privacy, the nature of their activities, and even their objectives. While some consider advocating for privacy as a way of preserving a basic human right, others frame it as a way to fight surveillance. Some organisations focus on the individual level, while others focus on the societal level. Some fight against a wide span of technologies, while others focus on specific intrusive technologies and practices (Bennett, 2008). Despite these differences, they are all united in their belief that even in the twenty-first century, privacy is not dead, and it is worthwhile to preserve it.

However, advocating for privacy is a challenge. In their privacy-related campaigns, organisations often find themselves isolated for two main reasons. First, during campaigns concerning other digital rights such as internet access, net neutrality, or the right to fair use, the interests of digital rights advocates have often coincided with those of powerful stakeholders, such as internet corporations or governments. This was evident in the campaign against the Stop Online Piracy Act and Protect IP Act (SOPA/PIPA) in the US (Benkler, Roberts, Faris, Solow-Niederman & Etling, 2013), and the protests against the Anti-Counterfeiting Trade Agreement (ACTA) in Europe (Losey, 2014). Yet when it comes to privacy, they have no interest in assisting civil society organisations in their goals *vis-à-vis* privacy rights, since governments and internet corporations have proven to use technological innovations in a manner that violates citizens' privacy either for security reasons or for financial and political gain (Greenwald, 2014; Rauhofer, 2008).

The second reason relates to the ability of civil society organisations to mobilise the public to their causes. To begin with, the decline in political and civic engagement (Norris, 2002) distances people from participating in the organisations' activities. Second, most citizens do not have sufficient knowledge or understanding of the topic (Livingstone, 2008; Osenga, 2013). This is of special importance when it comes to the right to privacy. Technological developments, along with violations committed by governments and internet corporations, have altered citizens' personal understanding and social expectations for privacy (Andrews 2012; Worthington, Fitch-Hauser, Välikoski, Imhof & Kim, 2011), so much so that the right to privacy might no longer seem important or relevant to most people. Finally, since most digital rights advocates subscribe to a Western viewpoint (Tăbușcă, 2010), non-Western countries may perceive them as hostile strategic communicators (Monroe, 2015). Thus, to achieve their goals, the organisations have to adjust their activities to fit the local society, or, to put it differently, learn how to sail against the wind.

Despite these obstacles, in the past decade there have been several successful privacy campaigns by digital rights advocates worldwide, as documented by EFF (2017a). For example, in 2005 in the UK, No2ID and its affiliates managed to derail a government plan for creating a biometric ID database (EFF, 2017b). In 2008, Derechos Digitales in Chile protected the privacy of internet users by opposing police plans for retrieving personal information about web commenters from internet corporations (EFF, 2017c). Finally, in 2012, OpenMedia.ca in Canada managed to put on hold online surveillance legislation (EFF, 2017d). This is not to say that these small victories have ended all privacy violations. However, each represents a reconstruction of the boundaries of privacy in these countries – if only for a short while. Against this background, I now turn to examining the way DRM coped with similar obstacles in Israel.

THE ISRAELI CASE: THE (NON)IMPORTANCE OF PRIVACY

When addressing privacy in Israel, one needs to take into consideration not only the legal right to privacy as enshrined in the country's legislation, but also the status of privacy as a cultural and social norm, since these two influence one another (Birnhack, 2010). A key cultural distinction in that regard is that between collectivism and individualism (Hofstede, 2001). In collectivist cultures, citizens are more likely to accept privacy intrusions in return for in-group belonging. Conversely, individualistic cultures are more concerned with online privacy because their citizens place higher value on private life and independence (Cho, Rivera-Sanchez, Lim, 2009; Milberg, Burke, Smith & Kallman, 1995).

Israel was established as a collectivist society: the value of privacy is thus not rooted in its culture, since it contradicts the culture of collectivism and the local ethos of sharing (Ribak & Turrow, 2003; Ribak, 2007). However, as a democratic state, despite its collectivist nature, the legal right to privacy in Israel is protected by law. First, according to Article 7 of *The Basic Law for Human Dignity and Liberty (1992)* which is part of the constitutional law of the country, everyone is entitled to privacy, then *The Protection of Privacy Law (1981)* which deals exclusively with the limits of the right to privacy in Israel. Second, there are several specific laws dealing with the right to privacy, among other issues, including *The Wiretap Law (1979)*; *The Basic Law: The Judiciary (1984)*; *Patients' Rights Act (1996)*; *The Criminal Procedure Law: Enforcement Powers – Body Search of Suspect (1996)* ; *The Freedom of Information Act (1998)* ; *The Prevention of Sexual Harassment Law (1998)* and *The Genetic Information Law (2000)*. Finally, in 2006, the Israeli government established The Israeli Law, Information, and Technology Authority and tasked it with strengthening the protection of personal data and tightening enforcement in cases of privacy violations. It is concerned with issues such as database protection, electronic signatures, and credit card information (Israeli Law Information and Technology Authority, 2017). However, socio-cultural norms in Israel lag far behind the legal normative public discourse (Karniel & Lavie-Dinur, 2012). Birnhack & Elkin-Koren (2009) demonstrate the gap by showing how most Israeli websites, including public and government websites, still do not provide users the adequate privacy protection as required by law.

This gap only widens when considered in the specific Israeli security context. Long before the digital revolution, Israel responded to security fears with laws and regulations that violate privacy in the name of national security (Ribak, 2003; Ribak & Turow, 2003). For example, according to *The Identity Card Carrying and Displaying Law (1982)*, all adult citizens are obligated to carry their government-issued ID card and must present it to any representative of the police or military on demand, even without probable cause. In addition, upon entering a public place, Israelis are often obliged to open their bags for security inspection and pass through a metal detector as their belongings are X-rayed (Israeli, 2013). Another example is the amendment to *The Criminal Procedure Law (Enforcement Powers – Communication Data (2007)* , which allows security agencies to acquire citizens' private communication data from internet and mobile service providers without any judicial oversight. Finally, in recent years, there has been a growing stream of legislation initiatives ostensibly designed to protect Israelis at the cost of violating citizens' privacy. The latest example is the Minister of Interior's initiative to compile a database of citizens who support the boycott, divestment, and sanctions (BDS) movement (Ravid, 2017).

Although these laws, regulations, and initiatives violate privacy on a regular basis, the annual

surveys of the Israeli Institute for Democracy indicate that most Israelis are willing to accept these violations, including online state surveillance, in exchange for security (Hermann, Heller, Cohen, Be'ery, & Lebel, 2015; Hermann, Heller, Cohen, & Bublil, 2016; Hermann, Heller, Cohen, Bublil & Omar, 2017).

The upshot is that the right to privacy in Israel is considered of limited importance: Israeli institutions are less sensitive to and Israeli citizens are more tolerant of violations compared to other Western societies, especially in exchange for personal security (Israeli, 2013; Shamah, 2013). As Ribak (2003, p. 20) puts it, privacy in Israel is "an unaffordable luxury that is willingly, unquestioningly surrendered and sacrificed". Thus, claims Ribak, it is no wonder that in Israel criticism of violations of privacy is rare. Nevertheless, as elaborated in the next section, the recent creation of a national biometric database did encounter resistance by Israeli civil society.

THE DRM: AIMING TO BE THE ISRAELI EFF

As in many countries, the Israeli government has initiated various well-meaning programmes that rely on surveillance and database technologies, which to some extent violate people's privacy. For example, the Credit Score Law (Zarhia & Izesko, 2015) provides lending institutions with access to financial information regarding future clients; City Without Violence involves widespread surveillance cameras deployment; and the National Traffic Management Centre involves installing surveillance cameras on highways and crossroads (City Without Violence, 2017; Netivei Israel, 2017). One of the largest and most controversial projects of this kind is T*he Inclusion of Biometric Means of Identification in Identity Documents and in an Information Database Law (2009).*

According to the law, each citizen is to be issued smart documents (ID card and passport) which include fingerprints and computerised tags of facial features. In addition, these biometric data are to be stored in encrypted form in a database supervised by the Biometric Database Management Authority (BDMA). As announced by the prime minister at the time, Ehud Olmert, the transition to smart ID and the creation of a biometric database served two purposes: reducing forgery and identity theft and providing better government services (Somfalvi & Ronen, 2008). The law provided for a two-year pilot in which the database was to operate on a trial basis and registration would be voluntary. During this period, the BDMA was tasked with examining the necessity of the database, designing measures of success, and looking into possible alternatives (due to possible violations of privacy). Only after this period was it to be decided whether to make it obligatory.

The initiative to establish the DRM came in 2009, in response to the creation of the biometric database. Its founders, whose expertise was mostly technological, feared the privacy implications of the database (Yaron, 2011). This led, in 2011, to the creation of the DRM as an official NGO dedicated to advocating for all digital rights. Prior to the establishment of the DRM, several civil society organisations in Israel – including the Association for Civil Rights in Israel (ACRI) and the Israel Internet Association (ISOC-IL) – had addressed digital rights among their other activities. Unlike them, however, the DRM distinguishes itself by dealing exclusively with digital rights (Yaron, 2011). As its founders declare, their aim is for the organisation to become the Israeli equivalent of the EFF. This ambition is manifested, for example, in the similarity between the organisations' founding declarations, both emphasising civil liberties and technology. The founders of the EFF define the aims of their organisation

thus:

The Electronic Frontier Foundation is the leading nonprofit organisation defending civil liberties in the digital world… We work to ensure that rights and freedoms are enhanced and protected as our use of technology grows. (EFF, 2017e)

And this is how the DRM defines its goals:

The DRM is engaged in protecting and promoting the rights of the individual and the community in the digital age. The organisation is engaged in protecting the right to privacy, freedom of expression, the right to equality, consumer rights, and the like, and relates to the possible infringement of these rights by information technologies… The organisation has set itself the goal to be a focal point of knowledge at points of interaction between technology and the rights of the individual and the community, and to promote those rights within the framework of its activities. (DRM, 2009a)

Interestingly, the similarities between the declarations also highlight the absence of any reference to local social or political aspects in the DRM's declaration: Israel is not mentioned either in the name of the organisation or in its declaration. This seemingly neutral declaration also marks the organisation as an apolitical entity. I will refer to this point again when analysing its activities vis-à-vis the biometric database.

At the time of writing, the DRM has begun to deal with issues like consumer rights and freedom of speech, but its main concern remains the right to privacy. So far, the organisation has documented and acted against six major privacy violations, mostly by government institutions. These include the Pet App, a database of dog owners created by the Ministry of Agriculture that exposed personal information (DRM, 2014a); the smartcard system for public transportation (DRM, 2011); and most importantly, the biometric database. This latter was the only violation to give rise to a full-scale campaign. Given the aforementioned challenges of civil society organisations when advocating for privacy, as well as the unique situation in Israel, this study asks: *What were the persuasion tactics used by the DRM in their campaign against the biometric database?*

METHODOLOGY

To answer the research question, I collected texts concerning DRM activities between the years 2009-2017. These materials included the organisation's official publications and announcements, retrieved from its website (n=22 documents); journalistic reports on the movement's work in 2009-2017 (n=76 documents); and minutes of the Joint Committee[1] (n=37 documents).

The analysis was carried out in two stages. The first entailed mapping all the actions taken by the DRM in 2009-2017, and the second involved analysing its arguments throughout the campaign. The analysis was based on the persuasion tactics typology suggested by Keck and Sikkink (1999) in their work on transnational advocacy networks, combined with Aristotelian definitions of modes of persuasion (Tausig, 2015). In what follows, I present the evolution of the campaign followed by an analysis of DRM's arguments.

CAMPAIGNING AGAINST BIOMETRICS: THREE ARENAS, THREE STORIES

Three arenas - From the beginning of the legislative process, the DRM opposed the law and began advocating against the database in three different arenas: political, judicial, and public. During the first stage of the campaign, the organisation focused on the political arena. Even before its official establishment, its activists had been engaged in lobbying and discussions about the legislation in various committees of the Knesset. One of the NGO's first official acts was to send a letter to Knesset members stressing the potential problems of the database in hopes of persuading them to vote against the law (DRM, 2009b). As the campaign progressed, members of the organisation continued their lobbying work at the political arena, participating in 26 out of 37 meetings of the Joint Committee meetings on the database (The Joint Committee, 2009-2017).

During the next stage, in 2012, the DRM operated in the judicial arena by appealing to the High Court of Justice to overrule the Knesset and abolish the biometric database (H.C. 1516/12, 2012). The court ruled that during the pilot stage there was no reason to abolish the database. However, it did rule that the DRM could re-appeal afterwards (Zarhin, 2012). Following the ruling, the pilot began in July 2013, and the state launched a massive media campaign encouraging people to join the database, claiming it would protect them against identity theft (Keinan & Zilber, 2013). Since the ads failed to mention that by doing so they would be joining the biometric database, the DRM appealed once again to the High Court of Justice to force the state to make full disclosure. The ruling in favour of the organisation received mainstream media coverage, which it used to publicise the controversy surrounding the database (Zarhin, 2012).

Furthermore, in response to the state's campaign, the organisation turned to the third arena, the mediated public sphere, and launched for the first time a social media campaign aimed at convincing people not to register for the database. Although during previous years its activists had continuously lobbied against the law in the public mediated arena, this was the first time they had mounted an official campaign. To finance the campaign, the DRM initiated a successful small-scale crowdfunding campaign to raise money to produce viral videos (DRM, 2013a). In January 2014, using the money it had raised, the organisation produced two such videos – "Why anti?" and "Why shouldn't you join the biometric database?" Their launch received mainstream media attention on a national scale, which helped DRM gain some public attention (Golan, 2014).

From that point on, the organisation continued to operate in all three arenas, recognising that in order to succeed they could not withdraw from any. For example, in February 2015, prior to a discussion in the Knesset, the BDMA published a partial report mapping the use of biometric databases around the world. In response, the DRM publicly crowdsourced a large-scale internet search for complete and accurate information on the matter, and publicised the information in various online media outlets (Lilien, 2015). In November 2016, the Ministry of Interior announced that following to the completion of the pilot stage, the database would become permanent and all Israeli citizens would be obligated to register. In response, the DRM initiated a combined campaign that included lobbying politicians (and encouraging citizens to reach out to members of Knesset asking them to vote against the database); launching another crowdfunding campaign to raise money for another appeal; interviews in various media outlets;

recruiting volunteers; and organising public meetings and demonstrations (Kabir, 2016). The use of all three arenas demonstrates the gradually growing efforts of the DRM to mobilize all relevant stakeholders.

Three stories - In all these arenas, the DRM attempted to persuade various stakeholders to act against the database. In their work on the persuasion tactics in transnational advocacy, Keck and Sikkink (1999) defined two tactics relevant to an analysis of the DRM's arguments: information politics and symbolic politics. The tactic of information politics relies on activists' ability to generate politically relevant information and to move it by the most effective means to the place it will have the most impact at the most critical time (Keck & Sikkink, 1999). Bennett (2008) elaborated on this tactic, reasoning that the politics of information in the context of privacy advocacy relies on the ability of privacy activists to produce reliable and accurate information about the possible harm caused by a certain intrusive technology or a new policy, for example by stressing its potentially hazardous consequences based on previous experience with similar surveillance systems at different times and places, or by arguing against its long-term ineffectiveness. In contrast, symbolic politics operates by evoking symbols, actions, values, beliefs, and stories so as to invest a situation with a meaning that resonates with a particular audience within a particular culture (Keck & Sikkink, 1999). By applying the Aristotelian modes of persuasion (Tausig, 2015) to the various stories of symbolic politics, I suggest that one can identify three venues of persuasion these stories trigger: logos (logic), ethos (the guiding beliefs of a person, group, or institution), and pathos (emotion).

In their work, Keck and Sikkink (1999) referred to each tactic separately; yet, when analysing the arguments raised by the DRM, it appears that each factual argument was backed up by a symbolic persuasion technique, whether explicitly or implicitly. The combination of both tactics created what I define as *cultural informational framing* (Daskal, 2017). This means that the organisation's arguments, as demonstrated below, were accurate and credible, but at the same time resonated with people's experiences, emotions, and knowledge, as well as with their socio-cultural expectations and norms.

1. Why the database should be abolished: because it's not necessary - As the organisation highlighted repeatedly throughout the campaign with the backing of cyber experts, there is a significant difference between issuing smart documents and creating a database. Issuing smart documents effectively solves the problem of stealing and forging official documents, but does it necessarily entail the creation of a database? The activists' answer is no: they declared that while they do support the transition to smart documents (passports and ID cards) for Israeli citizens, they object to the creation of a database due to its violation of citizens' privacy.

The right to privacy is essential in a democracy, thus the creation of the database will erode Israeli democracy. Based on the Aristotelian typology, by raising this argument, the organisation appealed to a key ethos in Israel: its pride in being a democratic state. This is how the argument was phrased in the organisation's letter to the Knesset members: "Collecting biometric features means that the state treats citizens as suspects… This is a disproportional assault on privacy, which is a fundamental right according to the Basic Laws of Israel" (DRM, 2009b, para. 3). The letter also stresses the importance of privacy in a democratic society by showcasing the Western perspective; it argues, "There are no such databases in any Western country… such a database would put Israel on the same plane as states such as Yemen, Pakistan, and Indonesia, which are not examples of enlightened regimes" (DRM, 2009b, para. 3). The same argument was brought to bear in the organisation's 2012 appeal to the High Court of Justice (H.C. 1516/12, 2012, p. 2):

"a biometric database… constitutes an unprecedented mechanism of control and surveillance. It inflicts severe and unnecessary harm to human dignity, its freedom and right to privacy. It undermines the basis of democracy".

2. Why the database should be abolished: because it's ineffective - Unlike the first argument, this argument justifies the database's abolition because it is ineffective. From an informational point of view, in its very first appeal to court in 2012, the organisation pointed out that the state had failed to carry out the actions required by law concerning the creation of the database: appointing an external monitor, establishing criteria for success, defining measures for testing reliability and validity, and evaluating alternatives for the biometric database (H.C. 1516/12, 2012). Later in the campaign, on at least four separate occasions, the organisation pointed out various shortcomings in the construction of the database which might damage its professional, safe, and secure functioning. For example, in June 2013, the DRM sent a letter to the Attorney General, claiming that the tender terms for securing the database contravened the law by allowing private companies to perform hacking tests on the database (DRM, 2013b). In March 2014, it again sent a letter to the Minister of Interior and the Minister of Justice asking them to delay the operation of the biometric database since the security confirmation was not yet complete (DRM, 2014b). Finally, in June 2015, the DRM published a special report that summarised all the problems and malfunctions of the database as analysed by cyber experts. The report's arguments (among others) were that

In 2014, 71 cases of phishing and forgery were discovered … Not one was prevented by a biometric database. The planning of the system is incorrect in several respects… The Biometric Authority did not examine alternatives that have worldwide credibility, and as for the alternatives that were examined, their results made no sense… Thus we call on the Israeli government and Members of Knesset to abolish the biometric database (DRM, 2015).

This last sentence captures nicely the symbolic frame that accompanies this argument – the logic perspective. By repeatedly pointing out the disparity between the law on paper and its application in practice during the pilot stage and the problems with the database, the activists invoked the logic of the politicians in trying to persuade them not to approve the database because it did not make sense.

3. Why the database should be abolished: because it will be breached - The final argument was that the database should be abolished because the government would not be able to guarantee protection against security breaches, and hence possible identity theft. This argument first appeared in the first letter addressed to Knesset members. In this letter, the DRM made the following statement: "Past experience and reports from the General Ombudsman have proved that State authorities cannot be trusted to maintain the security of the database" (DRM, 2009b, para. 4). In this sentence, the organisation set into motion both the Informational frame ("past experience and reports from the General Ombudsman") as well as the symbolic frame ("cannot be trusted").

In the judicial arena, within the framework of the appeal, the organisation explained the meaning of past experience and reinforced the informational frame. It wrote: "Past performance of the State in this field is not a source of pride: Not many countries in the world allow the downloading of sensitive census databases from sharing file sites, as is possible with the Israeli census" (H.C. 1516/12, 2012, p. 15). In addition, the activists also refer in the lawsuit to the leak of the adoption database, and the General Ombudsman reports critical of the state's failure to protect its citizens' privacy were also mentioned.

This symbolic frame concerning lack of trust was especially emphasised in the commercials the DRM produced as part of its publicity campaign. In the "Why anti?" commercial, a futuristic horror scenario was presented in which the biometric database leaked and the information fell into the hands of criminals. It showed a criminal using this information to track down a potential victim -a young woman in a pub. In the "Why shouldn't you join the biometric database?" commercial, a presenter delivered the message by again stressing the argument that the government could not be trusted with the private information of its citizens. It emphasised how each citizen could become a victim (of extortion or assault) if the database were to be breached, and it assured the audience that based on past experience (by specifically mentioning the state's inability to keep the information about Israel's nuclear reactor safe), it was likely to be breached. Thus, concluded the presenter, if you wish to maintain your privacy and your security, do not register.

Through this framing of privacy, the DRM tried to subvert the Israel equation according to which security means lack of privacy. In contrast, according to the campaign, only by holding on to your privacy can you secure yourself. Interestingly, despite the differences between the public campaigns of the government and the DRM, they both used the Aristotelian persuasion technique of Pathos, arousing the emotion of fear among the public: the former regarding identity theft, and the latter regarding the risk of criminals obtaining the information.

Overall, it can be seen that all of the arguments appeared in all of the arenas. However, one can distinguish between the first two arguments – which were specifically directed to the judicial and political arenas and were heard and seen in the mediated public sphere only because of media coverage – and the third argument, which was specifically directed to the mediated public sphere. This means that while in the political and the judicial arenas the DRM acknowledged the importance of privacy as a value in democracies, the problem of state surveillance in its work, and the technical as well administrative problems associated with the database, in the mediated public arena the organisation spotlights privacy in the context of personal security, lack of trust and governmental incompetence.

Since the second argument involves complex technical and administrative jargon, it is understandable why the organisation refrains from using it in the mediated public arena. After all, it was addressed mostly to the members of the Knesset who voted on the law, and not to the public. However, the decision to avoid the first argument and highlight the third in the mediated public sphere coincides with the local perspective, which values security over privacy as a democratic value, and does not trust the government (Hermann, Heller, Cohen, Be'ery, & Lebel, 2015; Hermann, Heller, Cohen, & Bublil, 2016; Hermann, Heller, Cohen, Bublil & Omar, 2017). Furthermore, in Israel, organisations which advocate for issues such as human rights, civil liberties, and democracy are usually considered to be on the left of the political map (for example, ACRI). Thus, framing the biometric database as a violation of civil rights, especially in the mediated public sphere, might alienate the public support of people from the centre and the right of the political map within the Israeli society. However, framing the biometric database in an apolitical frame, as in the third argument, blurs traditional political divisions and coincides with the neutral political position the DRM tries to maintain in order to increase its public support.

CONCLUDING REMARKS: EXPLORING THE NATIONAL MODELS OF PRIVACY GOVERNANCE

As mentioned above, on 30 November 2016, the Ministry of Interior declared that despite the criticism, the database would become obligatory for all Israeli citizens. On the same day, the DRM initiated another crowdfunding campaign (DRM, 2016). Within 24 hours, the target of about €15,000 was achieved. Furthermore, donations continued to arrive throughout the month: all told, some 1,000 people donated about €26,500. In comparison, the first crowdfunding campaign (DRM, 2013a) against the biometric database only drew 200 people who donated about €5,000. The results of this campaign indicate not only that DRM has begun to situate itself as a significant social actor in the Israeli society, but also that in the Israeli context, the issue of privacy grew in importance in the last few years, possibly due to the work of the DRM. As of now, the DRM has appealed to the high court to abolish the database by voicing all three arguments. Only time will tell if the movement will succeed in its campaign.

While focused on one case, important insights can be garnered from this study, concerning not only the role of civil society organisations in constructing privacy governance, but also its research. Digital rights are interpreted differently in every culture and society, but we must still differentiate the nature of these rights. For example, the meaning and boundaries of rights such as access to the internet and preservation of net neutrality are comparatively clear. While some stakeholders might object to defining them as rights to begin with, their meaning remains the same in different countries. In contrast, liberties such as the right to privacy and freedom of speech are more controversial, and their meaning and boundaries are inconsistent across cultures. Thus, when advocating for these rights in a given society, civil society organisations have to be flexible in the arguments they present and promote in order to achieve the political, public, and judicial support they need. The case of the DRM provides an example of such flexibility, which was manifested in three different cultural informational framings the organisation presented concerning the biometric database: the unnecessity of a biometric database in democracy; the database's ineffectiveness; and governmental incompetence in securing it. The organisation's ability to navigate between these arguments allowed it to maintain its image as a non-political organisation, which transcends political disagreements and possibly enables it to recruit more support to its cause.

While Israel's security situation is unique, it is not the only country whose government violates citizens' privacy in the name of security. In Europe, the refugee crisis and ISIS terrorist attacks have led to a series of various national legislative initiatives that infringe on citizens' civil liberties, not so different from the Israeli situation. For example, Germany, France, and the UK have passed laws granting their surveillance agencies autonomous power to conduct bulk interception of communications across Europe and beyond, almost without oversight. By doing so, they joined countries such as Poland, Austria, Italy, and Sweden, whose parliaments have already adopted extensive domestic and foreign surveillance legislation (Lubin, 2017). Yet at the same time, in these countries there are various civil society organisations which advocate for digital rights and against these legislative initiatives such as the Open Rights Group in the UK; La Quadrature du Net in France; Digitale Gesellschaft in Germany; Panoptykon Foundation in Poland; DFRI in Sweden; Initiative für Netzfreiheit (IfNf) in Austria, and many more. These organisations collaborate ad hoc regarding digital human rights issues in the regional context (Losey, 2014), and in 2002 over 30 civil rights organisations in Europe established the European Digital Rights (EDRI) advocacy group. Based in Brussels, it functions as an umbrella organisation, allowing for more systematic collaboration between the national organisations.

Follow-up studies in this direction might explore how organisations in these countries use different persuasion techniques in their campaigns for privacy and what power these techniques might have in the age in which "privacy is dead".

Finally, I wish to address the research of civil society campaigns within the broader perspective of privacy governance studies. Researching the point of view offered by a civil society organisation sheds light, from an emic point of view, on the existing boundaries of privacy governance as well as the perceived problematic aspect of these boundaries, in a given society. Furthermore, such line of inquiry can also reveal the kind of privacy governance. civil society wishes to create and its desirable boundaries. In this case, since the DRM focuses only on violations committed by political and public institutions, the model of privacy governance it is pursuing is based on protecting private information from political and public entities but not necessarily from internet corporations. This model is probably different from other models of privacy governance suggested by other civil society organisations in other countries, especially in Europe where internet corporations are more restricted in their work (Fioretti, 2017; Gibbs, 2017). Thus, following studies which define how national internet governance models are created such as the US or the Chinese model (Powers & Jablonski, 2015; MacKinnon, 2010), I would like to suggest a different avenue for future research that analyses and classifies models of national privacy governance based on the study of privacy advocates. Such analysis could help us understand more about the models of privacy governance that exist in a given society, how they are constructed and developed, how they can be modified, and why, sometimes, they will never change.

REFERENCES

Andrews, L. (2012). *I know who you are and I saw what you did: Social networks and the death of privacy*. New York, NY: Free Press.

Benedek, W. (2008). Internet governance and human rights. In W. Benedek, V. Bauer and M. Kettemann (Eds.) *Internet governance and the information society*. The Netherlands: Eleven International Publishing.

Benkler, Y., Roberts, H., Faris, R., Solow-Niederman, A. & Etling, B. (2013). *Social mobilization and the networked public sphere: Mapping the SOPA-PIPA debate*. Cambridge, MA: Berkman Center Research Publication. Retrieved from http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/MediaCloud_Social_Mobilization_and_the_Networked_Public_Sphere_0.pdf.

Bennett, C. (2008). *The privacy advocates: Resisting the spread of surveillance*. Cambridge, MA: The MIT press.

Birnhack, M. (2010). *Private space: The right to privacy, law and technology*. Israel: Bar Ilan University Press & Nevo Press.

Birnhack, M. & Elkin-Koren, N. (2009). Does law matter online? Empirical evidence on privacy law compliance, Social Science Research Network, August 5-46.

Breindl, Y. (2011). Promoting openness by "patching" European directives: Internet based activism & EU telecommunication reform. *Journal of Information, Technology and Politics, 8*(3), 346-366.

Cho, H., Rivera-Sanchez, M. Lim, S. S. (2009). A multidimensional study on online privacy: Global concerns and local responses. *New Media Society, 11*(3), 395-416.

City Without Violence, (2017). Municipal Command and Control Center. Retrieved from http://www.cwv.gov.il/Enforcement/Pages/MunicipalControlCenter.aspx

Daskal, E. (2017): Let's be careful out there … : How digital rights advocates educate citizens in the digital age. *Information, Communication & Society*. doi:10.1080/1369118X.2016.1271903

DeNardis, L. (2010). The Emerging Field of Internet Governance. *Yale Information Society Project Working Paper Series*. doi:10.2139/ssrn.1678343

DeNardis, L. & Raymond, M. (2013). Thinking clearly about Multistakeholder internet governance. Paper Presented at 8th Annual GigaNet Symposium Bali, Indonesia. Retrieved from http://www.phibetaiota.net/wp-content/uploads/2013/11/Multistakeholder-Internet-Governance.pdf

Digital Rights Movement (2009 a). *Who are we?* Retrieved from https://www.digitalrights.org.il/who/

Digital Rights Movement (2009 b). The digital rights movement is calling for the members of the Knesset to vote in favour of the reservations from the creation of a central biometric database. Retrieved from https://www.digitalrights.org.il/2009/11/%D7%94%D7%95%D7%93%D7%A2%D7%94-%D7%9C%D7%A2%D7%99%D7%AA%D7%95%D7%A0%D7%95%D7%AA-151109/

Digital Rights Movement (2011). Position paper about the "Rav Kav" cards. Retrieved from https://www.digitalrights.org.il/2011/06/%D7%A0%D7%99%D7%99%D7%A8-%D7%A2%D7%9E%D7%93%D7%94-%D7%91%D7%A0%D7%95%D7%92%D7%A2-%D7%9C%D7%9B%D7%A8%D7%98%D7%99%D7%A1%D7%99-%D7%94%D7%A8%D7%91-%D7%A7%D7%95/

Digital Rights Movement (2013 a). Crowdfunding for a campaign against the biometric database. Retrieved from https://www.digitalrights.org.il/2013/08/%D7%9E%D7%99%D7%9E%D7%95%D7%9F-%D7%94%D7%9E%D7%95%D7%A0%D7%99%D7%9D-%D7%9C%D7%A7%D7%9E%D7%A4%D7%99%D7%99%D7%9F-%D7%A0%D7%92%D7%93-%D7%94%D7%9E%D7%90%D7%92%D7%A8-%D7%94%D7%91%D7%99%D7%95%D7%9E%D7%98/

Digital Rights Movement (2013 b). The Digital Rights Movement: the biometric database authority privatises the database information. Retrieved from https://www.digitalrights.org.il/2013/06/%D7%A4%D7%A0%D7%99%D7%99%D7%94-%D7%9C%D7%99%D7%95%D7%A2%D7%A5-%D7%94%D7%9E%D7%A9%D7%A4%D7%98%D7%99-%D7%9C%D7%9E%D7%9E%D7%A9%D7%9C%D7%94-%D7%91%D7%A0%D7%95%D7%92%D7%A2-%D7%9C%D7%9E%D7%90%D7%92%D7%A8/

Digital Rights Movement (2014 a). Personal details leaked through the "dogs database" application of Ministry of Agriculture. Retrieved from https://www.digitalrights.org.il/2014/11/%D7%A4%D7%A8%D7%98%D7%99%D7%9D-%D7%90%D7%99%D7%A9%D7%99%D7%99%D7%9D-%D7%93%D7%9C%D7%A4%D7%95-%D7%93%D7%A8%D7%9A-%D7%90%D7%A4%D7%9C%D7%99%D7%A7%D7%A6%D7%99%D7%99%D7%AA-%D7%9E%D7%90%D7%92%D7%A8/

Digital Rights Movement (2014 b). The Digital Rights Movement approached the Ministry of Interior for lack of sufficient security standards. Retrieved from https://www.digitalrights.org.il/2014/03/%D7%94%D7%9E%D7%90%D7%92%D7%A8-%D7%94%D7%91%D7%99%D7%95%D7%9E%D7%98%D7%A8%D7%99-%D7%90%D7%99%D7%A0%D7%95-%D7%A2%D7%95%D7%9E%D7%93-%D7%91%D7%AA%D7%A7%D7%A0%D7%99-%D7%94%D7%90%D7%91%D7%98%D7%97%D7%94/

Digital Rights Movement (2015). Experts' report of the Digital Rights Movement: a fear for a deliberate omission of information and an attempt to mislead the members of the Knesset and the public by presenting false information concerning the biometric database. Retrieved from https://www.digitalrights.org.il/2015/06/%D7%94%D7%AA%D7%A0%D7%95%D7%A2%D7%94-%D7%9C%D7%96%D7%9B%D7%95%D7%99%D7%95%D7%AA-%D7%93%D7%99%D7%92%D7%99%D7%98%D7%9C%D7%99%D7%95%D7%AA-%D7%9E%D7%A4%D7%A8%D7%A1%D7%9E%D7%AA-%D7%93%D7%95%D7%B4%D7%97/

Digital Rights Movement (2016). Crowdfunding for a high court appeal to abolish the biometric database. Retrieved from https://www.digitalrights.org.il/2016/11/%D7%92%D7%99%D7%95%D7%A1-%D7%94%D7%9E%D7%95%D7%A0%D7%99%D7%9D-%D7%9C%D7%9E%D7%A2%D7%9F-

%D7%91%D7%92%D7%B4%D7%A5-%D7%9C%D7%94%D7%A4%D7%9C%D7%AA-%D7%94%D7%9E%D7%90%D7%92%D7%A8-%D7%94%D7%91%D7%99%D7%95/

Electronic Frontier Foundation, (2017 a). *Counter-Surveillance Success Stories*. Retrieved from https://www.eff.org/csss

Electronic Frontier Foundation, (2017 b). *Success Story: Dismantling UK's Biometric ID Database*. Retrieved from https://www.eff.org/pages/success-story-dismantling-uk%E2%80%99s-biometric-id-database

Electronic Frontier Foundation, (2017 c). Success Story: Protecting Privacy of Web Commenters (Chile). Retrieved from https://www.eff.org/pages/success-story-protecting-privacy-web-commenters-chile

Electronic Frontier Foundation, (2017 d). *Success Story: Turning the Tide Against Online Spying*. Retrieved from https://www.eff.org/pages/success-story-turning-tide-against-online-spying

Electronic Frontier Foundation, (2017e). *About EFF*. Retrieved from https://www.eff.org/about

Fernández Pérez, M. (2015). *The final countdown for net neutrality in the EU*. EDRi. Retrieved From https://edri.org/the-final-countdown-for-net-neutrality-in-the-eu/

Fioretti, J. (2017, July 24). EU increases pressure on Facebook, Google and Twitter over user terms. *Reuters*. Retrieved from http://www.businessinsider.com/r-eu-increases-pressure-on-facebook-google-and-twitter-over-user-terms-2017-7

Gibbs, S. (2017, January 10). WhatsApp, Facebook and Google face tough new privacy rules under EC proposal. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2017/jan/10/whatsapp-facebook-google-privacy-rules-ec-european-directive

Golan, A. (2014, February 2). A virtual campaign was launched against the biometric database. *Nrg*. Retrieved from http://www.nrg.co.il/online/13/ART2/548/154.html?hp=13&cat=131&loc=51 [Heb].

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state*. New York, NY: Metropolitan Books.

H.C. 1516/12 (2012). *Nahon v. the Knesset*. Retrieved from http://www.acri.org.il/he/wp-content/uploads/2012/02/hit1516.pdf

Hermann, T., Heller, E., Cohen, C., Be'ery, G., & Lebel, Y. (2015). *The Israeli Democracy Index 2014*. Israel: The Israel Democracy Institute. Retrieved from https://www.idi.org.il/media/3667/democracy_index_2014.pdf [Heb].

Hermann, T., Heller, E., Cohen, C., & Bublil, D. (2016). *The Israeli Democracy Index 2015*. Israel: The Israel Democracy Institute. Retrieved from https://www.idi.org.il/media/3573/democracy_index_2015.pdf [Heb].

Hermann, T., Heller, E., Cohen, C., Bublil, D. & Omar, F. (2017). *The Israeli Democracy Index*

2016. Israel: The Israel Democracy Institute. Retrieved from https://www.idi.org.il/media/7799/democracy-index-2016.pdf [Heb].

Hofstede, G. (2001). *Culture's consequences: Comparing values, behaviors, institutions and organizations across nations*. Thousand Oaks, CA: Sage Publications.

Israeli, T. (2013). Who is afraid of "Google": Attitudes towards privacy on-line. *Mida'at, 9*, 28-45 [Heb].

Israeli Law Information and Technology Authority (2017). About The Israeli Law, Information and Technology Authority. *Ministry of Justice*. Retrieved from http://www.justice.gov.il/Units/ilita/Odot/Pages/Odot.aspx

Kabir, O. (2016, November 30). The digital rights movement will appeal to the high court against the biometric database decision. *Calcalist*. Retrieved from https://www.calcalist.co.il/internet/articles/0,7340,L-3702896,00.html [Heb].

Karniel, Y. & Lavie□Dinur, A. (2012). Privacy in new media in Israel: How social networks are helping to shape the perception of privacy in Israeli society. *Journal of Information, Communication and Ethics in Society*, 10(4), 288-304. doi:10.1108/14779961211285908

Kay, M. (2014). Human rights for the digital age. *Journal of Mass Media Ethics, 29*(1), 2-18.

Keck, M. E. & Sikkink, K. (1999). Transnational advocacy networks in international and regional politics. *International Social Science Journal, 51*, 89-101.

Keinan, I & Zilber, J. (2013, October 9). The biometric database: Payed talkbackers and product placement on the way to smart ID. *Haaretz*. Retrieved from https://www.haaretz.co.il/captain/room404/.premium-1.2136462 [Heb].

Kosoff, M. (2017, May 18). The battle to save the internet from Trump begins. *Vanity Fair*. Retrieved from https://www.vanityfair.com/news/2017/05/inside-the-battle-to-save-the-internet-from-donald-trump

Kulesza, J. (2008). Freedom of information in the global information society – the question of The Internet Bill of Rights, *UWM Law Review*, 1, 81 – 95. doi:10.2139/ssrn.1446771

Lilien, N. (2015, February 11). Where in the world are there biometric databases? *The Uplink: A Hebrew technology magazine*. Retrieved from https://www.lnk.co.il/shorty/world-biometric-database [Heb].

Livingstone, S. (2008). Internet Literacy: Young people's negotiation of new online Opportunities. In T. M. (Eds.), *Digital Youth, Innovation, and the unexpected* (pp. 101-122). Cambridge: The MIT Press.

Losey, J. (2014). The Anti-Counterfeiting Trade Agreement and European civil society: A case study on networked advocacy. *Journal of Information Policy*, 4, 205-227.

Lubin, A. (2017, January 9). A New Era of Mass Surveillance is Emerging Across

Europe. *Just Security*. Retrieved from https://www.justsecurity.org/36098/era-mass-surveillance-emerging-europe/.

Lessig L. (2006). Code is law: On liberty in cyberspace. *Harvard Magazine*. Retrieved from http://harvardmagazine.com/2000/01/code-is-law-html

MacKinnon, R (2010). *Networked Authoritarianism in China and beyond: Implications for Global Internet Freedom (White paper)*. CA: Stanford University. Retrieved from http://fsi-media.stanford.edu/evnts/6349/MacKinnon_Libtech.pdf.

Milberg, S. J., Burke, S. J., Smith, J. H., & Kallman, E.A. (1995). Rethinking copyright issues and ethics on the net: Values, personal information privacy, and regulatory approaches. *Communications of the ACM, 38*(12), 65-73.

Monroe, E. P. (2015). *Free expression, globalism and the new strategic communication*. UK: Cambridge University press.

Mueller, M. L. (2010). *Network and States: The Global Politics of Internet Governance*. MA: MIT press.

Netivei Israel (2017). National Traffic Management Center. Retrieved from https://www.iroads.co.il/en/content/national-traffic-management-center

Newman, A. (2008). *Protectors of privacy: Regulating personal data in the global economy*. Ithaca: Cornell University Press.

Norris, P. (2002). *Democratic Phoenix: Reinventing Political Activism*. New York: Cambridge University Press

Osenga, K. J. (2013). The internet is not a super highway: Using metaphors to communicate information and communications policy. *J. Info. Pol'y*, 3, 30-54.

Panwar, P. (2015, April 15). Know all about #netneutrality in India & save the internet: Explained. *OneIndia* Retrieved from http://www.oneindia.com/feature/know-what-is-net-neutrality-and-save-the-internet-explained-1713980.html

Patient's Rights Act (1996). *Knesset Israel,* 1591:327-336. Retrieved from http://fs.knesset.gov.il//13/law/13_lsr_211755.PDF

Postigo, H. (2008). Capturing fair use for the Youtube generation: The digital rights movement, the Electronic Frontier Foundation, and the user-centered framing of fair use. *Information, Communication & Society, 11*(7), 1008-1027.

Powers, S. M. & Jablonski, M. (2015). *The real cyber war: the political economy of Internet Freedom*. IL: University of Illinois Press.

Ravid, B. (2017, March 21). Israeli ministry trying to compile database of citizens who support BDS. *Haaretz*. Retrieved from http://www.haaretz.com/israel-news/1.778516 [Heb].

Rauhofer J. (2008). Privacy is dead, get over it! Information privacy and the dream of a risk-free society. *Information & Communications Technology Law*, *17*(3), 185-197.

Regan, P. M. (1995) *Legislating Privacy: Technology, Social Values, and Public Policy*. Chapel Hill: The University of North Carolina Press.

Ribak, R. (2003, May). *Parents' concerns over the internet: A cross-cultural comparison*. Paper presented at the annual meeting of the International Communication Association, San Diego, CA. Retrieved from http://www.allacademic.com/meta/p112185_index.html

Ribak, R. (2007). Privacy is a basic American value: Globalization and the construction of web privacy in Israel. *Communication Review, 10*(1), 1-27.

Ribak, R. & Turow, J. (2003). Internet power and social context: A globalization approach to web privacy concerns. *Journal of Broadcasting & Electronic Media,* 47(3), 328-349.

Shamah, D. (2013, June 9). Israelis are used to being spied on all the time. *The Times of Israel*. Retrieved from http://www.timesofisrael.com/israeli-authorities-use-far-wider-surveillance-powers-than-those-causing-storm-in-us/ [Heb].

Solove, D. J. & Hartzog, W. (2014). The FTC and the New Common Law of

Privacy. *Columbia Law Review,* 114, 583-676.

Somfalvi, A. & Ronen, E. (2008, August 3). The government approves: Biometric database for Israeli citizens. *Ynet*. Retrieved from http://www.ynet.co.il/articles/1,7340,L-3576961,00.html [Heb].

Tăbuşcă, S. M. (2010). The internet access as a fundamental right. *Journal of Information Systems and Operations Management*, 4(2), 206 – 212.

Tausig, D. (2015). Living proof: Autobiographical political argument in We Are the 99 Percent and We Are the 53 Percent. *International Journal of Communication*, 9, 1256–1274

The Basic Law: Human Dignity and Liberty (1992). *Knesset Israel*, 1391, 150. Retrieved from http://fs.knesset.gov.il/12/law/12_lsr_211801.PDF

The Basic Law: The Judiciary, (1984). *Knesset Israel,* 1123, 198-218. Retrieved from http://fs.knesset.gov.il/11/law/11_lsr_311021.PDF

The Criminal Procedure Law (Enforcement Powers – Body Search of Suspect), (1996). *Knesset Israel,* 1573: 136-149. Retrieved from http://fs.knesset.gov.il/13/law/13_lsr_211315.PDF

The Criminal Procedure Law (Enforcement Powers – Communication Data), (2007). *Knesset Israel,* 2122: 72-78. Retrieved from http://fs.knesset.gov.il/17/law/17_lsr_300150.pdf

The Freedom of Information Act, (1998). *Knesset Israel,* 1667, 226-232. Retrieved from http://fs.knesset.gov.il/14/law/14_lsr_211487.PDF

The Genetic Information Law, (2000). *Knesset Israel,* 1766, 62-74. Retrieved from http://fs.knesset.gov.il/15/law/15_lsr_300291.pdf

The Identity Card Carrying and Displaying Law, (1982). *Knesset Israel,* 1070: 20. Retrieved from http://fs.knesset.gov.il//10/law/10_lsr_210028.PDF

The Inclusion of Biometric Means of Identification in Identity Documents and in an Information Database Law (2009). *Knesset Israel,* 2217, 255-272. Retrieved from http://fs.knesset.gov.il/18/law/18_lsr_300928.pdf

The Joint Committee of the Science and Technology Committee and the Interior and Environmental Protection Committee protocols (2009-2017). *The official protocols of the Knesset*. Retrieved from http://main.knesset.gov.il/Activity/Legislation/Laws/Pages/lawlaws.aspx?t=lawlaws&st=lawlaws

The Prevention of Sexual Harassment Law, (1998). *Knesset Israel,* 1661: 166-170. Retrieved from http://fs.knesset.gov.il/14/law/14_lsr_211481.PDF

The Protection of Privacy Law (1981). *Knesset Israel,* 1011: 128-134. Retrieved from http://fs.knesset.gov.il//9/law/9_lsr_208332.PDF

The Wiretap Law (1979). *Knesset Israel,* 938: 118-120. Retrieved from http://fs.knesset.gov.il//9/law/9_lsr_208328.PDF

Worthington D., Fitch-Hauser, M., Välikoski, T.R., Imhof, M. & Kim, S.H. (2011). Listening and privacy management in mobile phone conversations: A cross-cultural comparison of Finnish, German, Korean and United States students. *Empedocles: European Journal for the Philosophy of Communication, 3*(1), 43-60.

Yaron, O. (2011, August 12). Fighting to keep privacy alive. *Haaretz*. Retrieved from http://www.haaretz.co.il/captain/net/1.1372639 [Heb].

Zarhin, T. (2012, July 23). Justices of the High Court of Justice: The necessity of the biometric database should be examined. *Haaretz*. Retrieved from http://www.haaretz.co.il/news/law/1.1783741 [Heb].

Zarhia, T. & Izesko, S. (2015, September 6). The law that will change the credit market. *TheMarker*. Retrieved from http://www.themarker.com/news/1.2725229 [Heb].

FOOTNOTES

1. The Joint Committee is a parliamentary committee formed by the Knesset (the Israeli parliament) to deal with the biometric database.