Privacy in an Era of Change

Introduction

Discussing the right to privacy is, to a great extent, like entering into a fog. Controversies can be found with regard to almost every aspect of this right and the extent of protection it warrants, whether on the normative plane or on the conceptual plane. There are those who view it as a demand and others who view it as a right, an interest, a value, a preference or an existential state. Protecting privacy is therefore perceived in several different ways: as a descriptive concept, as a normative concept, as a legal concept, or as all three. The principle of privacy in itself stems from worldviews concerning government, human rights, relations between individual and state, and relations between the public arena and private space. It can be assumed that the controversies stem, at least partially, from the fact that the discussion about the right to privacy, like its constitutional anchoring and the anchoring of the institutional arrangements related to it, developed relatively late in comparison to other rights.

In Israel as well—where the right to privacy is anchored in the Basic Law: Human Dignity and Liberty and in the Privacy Protection Act—the right to privacy has not been precisely defined in law or in case law. The Privacy Protection Act does not define its scope, but instead lists 11 actions that are considered infringements of privacy. They include: surveillance of a person in a manner likely to harass them, wiretapping prohibited by law, photographing a person in a private domain and infringing an obligation of secrecy in respect of a person's private affairs. Although Israeli law has embraced a broad definition of the concept of privacy, "the interest of an individual not to be harassed by others in his private life,"[1] the court has emphasized that the scope of the right is unclear and is subject to change in accordance with reality.[2]

One aspect of the right to privacy is the right of every person to maintain and protect their identity and a protective space surrounding their body, thoughts, feelings, innermost secrets, lifestyle and intimate acts. This aspect stems from the perception of privacy as an essential

---

[1] Civil Appeal 1211/96 Cohen v. National Consultants (1997).

[2] HCJ 2481/93 Dayan v. Wilk (1994).

component of maintaining one's identity and forming loving relationships, closeness and trust with those surrounding us, in addition to one's political, public identity. Not in vain was the loss of privacy thought of in the past as the tragedy of a totalitarian, inhumane society. Another aspect relates to the possibility that the right to privacy allows a person to choose the areas and places in his or her private domain where access is provided to others and to control the manner of exposure, its scope and timing.

Thus, in a different, more extreme manner than with regard to other human rights, the right to privacy is one whose limits, contexts and the norms derived from its protection remain undefined. Moreover, in recent years, the tension and clashes between the familiar values of the past and contemporary practices have reached new heights.

In a groundbreaking article concerning recognition of the right to privacy published in the Harvard Law Review in 1890, two young lawyers—later to become United States Supreme Court Justices, Samuel Warren and Louis Brandeis—wrote that modern enterprise and invention have subjected the individual to mental pain and distress.[3] The authors of the article were referring to the then advanced technology of mobile cameras which, for the first time, enabled journalists and press photographers to photograph people without their consent. Some one hundred and twenty years later, information technologies are perceived as the principal threat to privacy since they enable transfer of data worldwide at the speed of light. The accessibility of the internet, the emergence of social networks, the distribution of cellular devices, and the abundance of cameras installed in the public domain are bringing about significant changes in the meaning and scope of the expectation of privacy, and, as a result, the scope of the right to privacy. It was for good reason that the CEO of Google Corporation and, later, the founder of Facebook stated on various occasions that in the era of the internet and social networks, privacy is dead.[4] In practice, privacy is one of the most urgent social topics associated with digital communication technology.

The principle of protecting privacy as an accumulation of rights has various aspects which connect to various technologies. Indeed, government databases are quite unlike the internet, cellular phones and other portable devices, biometric databases, social networks, data

---

[3] S. Warren and L. Brandeis, "The Right to Privacy," *Harvard Law Review* 4/5 (1890): 193–213 http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

[4] http://www.guardian.co.uk/technology/2010/jan/11/facebook-privacy

mining and other technologies. At the end of November 2011, the Wikileaks site published a new collection of documents it called "the spy files,"[5] which included documents, presentations, contracts and catalogs of corporations offering surveillance, censorship, intelligence and security services, such as Siemens, HP, and the Israeli company NICE. In most cases, the material related to services and products sold directly to governments and intelligence agencies and not to the general public. NICE, for example, markets a variety of "intelligence solutions" including a platform for the interception and analysis of very large quantities of communication information, such as phone calls or Web surfing. According to the document, this system can, among its other functions, identify suspicious targets by scanning billions of voice conversations, texts and additional data. In a post 9/11 world, such systems are routinely purchased.

The reasonable expectation of privacy protection relates, first and foremost, to the relationship of the individual and government, and to the possibility that government may misuse technologies which can potentially infringe privacy. The fact that phone companies keep records of all calls, as do all cellular operating companies, is not a new phenomenon. In fact, the authorities use these records when they request search warrants or wiretapping permits from the courts. However, the discussion no longer relates to security cameras at malls or cross-border satellites. In the past decade, giant commercial entities are becoming information miners. While governments aspire to keep track of details, information and data based corporations such as Google or Facebook glean information regarding those details and store them on their servers, which are mostly located in the United States. One of the practices increasing tension between technology and the right to privacy is data ubiquity. New, inexpensive technologies for collection, storage, and analysis of data have dramatically increased in the past decade. It can be said—using a term borrowed from the European Union's data protection directive—that we are all, in fact, "data subjects."

The issue of location-based applications, the "cousin" of information-based advertising, can serve as a representative example. In order to activate a location-based application (finding a restaurant, movie theater, gas station or weather forecast, as well as verifying the local time), the device must know the user's location. This is accomplished by various methods, such as triangulation from cellular towers or utilization of a GPS chip embedded in the device. However, the information regarding the precise location of a user at a given time is not of high value in

[5] http://wikileaks.org/the-spyfiles.html

itself. Integration of hyper-private information with a location can render a location-based application valuable to its users and improve user experience. These types of information can be, for example, behavior and location in the past (What were the most recent searches on that area's foursquare? Where was the car parked most recently? How many tweets came in from the area?), shopping preferences, credit card status and recent transactions made with it.

As activity on the Web becomes more personal and as the uses of the Web move toward personal ones ("Me Centered Web"),[6] more third parties are looking to earn money by using the free tools we have been provided with to communicate and share information. Corporations such as Klout and PeerIndex would like to draw simple numbers out of the complex array of social networks as a whole, which would then be attached to each and every one of us, whether or not we want them to be. The situation in which every person has a "number"—an impact factor which reflects the impact he or she has—is not a fictional one. The difficulty in this situation is that the number will determine whether we get a job, a hotel room upgrade, a supermarket sale sample, a loan or anything else.

Even if values of "decision privacy"—meaning the freedom to make decisions in private matters, such as sexual orientation or the right to have an abortion, as well as the sense of local privacy (i.e., exercising control over actual private space, such as a house or courtyard)—seem relatively protected and conventional, when it comes to information privacy, things become more complicated.

Furthermore, data mining technologies raise serious questions about the very distinction between private and public. On the one hand—private enterprises and applications thrive on public information and derivatives of information gathered by the government, and on the other—public authorities make use of information mined by private companies (for example, by monitoring email correspondence between individuals). Moreover, the general public relies paradoxically on the assumption that it is the state that will protect them from misuse of their private information when technologies become cheaper or are frequently used by commercial corporations. Simultaneously, the public relies on private corporations and watchdog organizations external to the government to protect them from being harmed by the state.

---

[6] http://scholarlykitchen.sspnet.org/2010/10/26/rethinking-our-architecture-the-power-of-me-vs-the-arrogance-of-we/

An issue of concern is the extent to which privacy protection lags behind data collection systems and technologies used for tracking surfers in order to analyze and earn secondary profits from them. In an attempt to deal with a carefully orchestrated infringement of privacy—not by the state but on the part of commercial corporations—the privacy protection commissioners in Europe and Israel are trying to enforce information protection laws that were enacted and designed in another era, before Google and Facebook were born. But embracing new technologies compels regulators and legislators to play cat-and-mouse games. Legislation in most Western countries lacks the requisite tools for dealing with the international context of the storage and extraction of information, and this adversely affects the efficiency of European or Israeli authorities coping with corporations domiciled in the United States.

As a rule, it is not surprising that the history of legislation regarding privacy is of a reactive nature. An abundance of examples can be provided from the world over, from rules relating to the transmission of credit history in the seventies, to borrowing films on video libraries in the eighties, to accessing medical records in the nineties all the way to user conditions which enable internet companies to transfer personal details to offline companies in the early 2000s. It seems that a pattern of conduct can be outlined: A researcher, expert, or hacker discovers that a service or product which has a very broad circulation has a breach in its security or a component which enables the infringement of users' privacy. This assertion is affirmed by additional Web experts. Representatives of the company use a multi-level marketing strategy which begins with an unequivocal denial, moves on to an explanation, and ends with an apology and a declaration that the problem will be fixed and the infringement removed. Finally, a political-regulatory-legal reaction arrives: a governmental petition to the companies requesting clarifications, hearings in houses of representatives and other regulatory agencies, position papers and policy decisions, suggestions for legislative amendment, and the filing of class action lawsuits.

This is what occurred when, in early 2011, it was discovered that Apple Corporation is able to follow the movements of the users of cellular devices it markets, and in practice, even performs this surveillance using a non encrypted method.[7] This is what occurred in the matter of TomTom Corporation as well, after it was discovered that the company was selling information

[7] http://www.guardian.co.uk/technology/2011/apr/20/iphone-tracking-prompts-privacy-fears

it had collected through the GPS devices it manufactures[8] to the German police for the purpose of surveillance of traffic law violators.

The regulatory response of the American Federal Trade Commission regarding the usage of techniques for collecting and mining information on the Web was published in the middle of 2011. The FTC determined that the techniques constituted a severe infringement of user privacy. The paper included recommendations for users to improve their control information pertaining to their digital behavior and required companies to integrate a "privacy cookie" in their programs that would enable surfers to activate a "don't follow me" mechanism. This mechanism was supposed to have handed the users' private preferences over to information mining companies.

However, the number of these episodes is increasing, and it seems that they are becoming more and more severe. At the beginning of December 2011, an American security researcher discovered tracking software by the name of Carrier IQ installed in 140 million smart phones worldwide. The software follows almost every use, sound, and typing, copies it and transfers it back to the telecom companies. This tracking doesn't relate to the physical location of the device alone, but even to the content transmitted through it. This activity involved almost all the large manufacturers of this type of phone worldwide, e.g., Samsung, Nokia, Motorola, and Apple.[9] Following denials on part of those involved, a new PR tactic was unveiled, claiming that the application is used to monitor the device's performance, and is not used for surveillance purposes. It is difficult to deny that this sort of software is a gateway to a treasure chest of personal information regarding browsers' habits and movements. On the other hand, when technology advances and what becomes a "trail of breadcrumbs" for those performing the surveillance is the device itself, not one type of software or another, it becomes clear that we are not dealing with a problem that can be solved by the proposed method of opting out[10] suggested by the FTC. It can be assumed that when, one day, an additional report is published the need to deal with new aspects of the issue will arise.

---

[8] http://www.guardian.co.uk/technology/2011/apr/28/tomtom-satnav-data-police-speed-traps

[9] A. Kabir and H. Eilam, "All the Data is Recorded and Saved: Tracking Scandals of the Technological World" ynet, Kalkalist, 4.12.11 (Hebrew) http://www.calcalist.co.il/internet/articles/0,7340,L-3554064,00.html

[10] I.e., the system is valid, but the option of making exceptions is provided.

In her book "Privacy in Context,"[11] Helen Nissenbaum claims that people are not interested in restricting the stream of information, but rather in ensuring that the information is streaming in properly, in a way she calls contextual integrity. She claims that the right to privacy is not the right to control personal information nor is it the right to limit access to this information. The right to privacy is, in her opinion, the right to live in a world where our expectations regarding our personal information are both respected and responded to. These expectations are formed not just by habit, but by the force of trust in the support and recognition lent to them by social and political principles. Nissenbaum's view corresponds doubtlessly with what courts, especially in the United States, view as "reasonable expectation of privacy." Just as reasonable expectation as a legal doctrine is determined in other contexts, at least in part, in accordance with reality, so would it be difficult to claim that a certain act constituted a violation of reasonable expectation if the practice is one that is accepted socially. This is the case with regard to matters of technology and privacy as well. The open question is, therefore, twofold. Firstly, at what point can it be said that society has embraced a new technology, to the degree that it can no longer be claimed that one had a reasonable expectation that the technology would not be employed? Secondly, is it correct and justified—in a normative sense— to forego the reasonable expectation of personal information privacy in certain cases?

Peter Fleischer, former supervisor of international privacy at Google, wrote that the demand for privacy is "the new black in censorship fashion" and that this demand negates the principle of freedom of expression. He claims that the fact that privacy doesn't exist should be internalized, and that anyone looking for privacy probably has something to hide.[12] It is difficult to ignore the fact that the support of companies like Google for freedom of expression in this context stems from their economic model. Metaphorically, one could argue that the right to freedom of expression is the "new black" in information mining fashion. Therefore, it seems that the main question relates to profit and loss with regard to gathering information: Are we prepared to accept the advantages of location-based services at the expense of our privacy? Are we interested in maintaining a space where our actions are not measured, or do we prefer the

---

[11] H. Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford: Stanford University Press, 2010).

[12] http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html

advantages of the measurement and monitoring of every act while integrating types of data? (For example: Is the exercise I did equal in value to my calorie intake; was my daughter sick too many times this winter; do I spend more money on shoes relative to others with a similar salary?)

A question no less worrying is whether it is at all possible to discuss profit and loss on the normative plane when in practice the process seems to be unstoppable. It is possible that history itself will judge this—especially if those below the social-technological gap (namely, those under 40 years of age) exhibit indifference toward privacy issues. Simultaneously, it is possible that sufficient public pressure will succeed in leading to a situation where privacy issues on online media and beyond will become huge public campaign issues. No one likes the concept of a "Big Brother," and it can be assumed that corporate giants like Google, Apple, and Microsoft will become easy targets due to their power.

This book is the outcome of several years of work. Two of the articles are the products of research conducted within the Israel Democracy Institute, and two others resulted from a call for papers we published regarding a book on the topic of privacy and journalism. More than anything, the anthology reflects the many faces of the right to privacy, and the transition period this right is undergoing—from traditional media to new media; from ethical and legal practices whose purpose is to infringe privacy through programs watched by the masses to the infringement of individual privacy in the digital world.

Due to a strong sense that things are the same everywhere and that nothing is new under the sun, bewildered legislators at the advent of the twenty-first century are returning to basic axioms of privacy protection from the early twentieth century. **Re'em Segev**'s article relates to these axioms in the context of the privacy concept. With a complex, ambiguous view of the concept, Segev explores whether privacy should be defined as a situation of isolation (e.g., a situation where data concerning a person is unknown to others) or as the extent to which a person can control his or her degree of isolation from others (e.g., the extent to which data concerning him or her is known to others). Segev also grapples with the question of whether to maintain a uniform perception of privacy or to adopt a variety of perceptions depending on personal characteristics or the cultural framework in which people live. He also critiques what is perceived as an underlying assumption of Israeli courts and court systems in other countries whereby privacy ends where its relinquishment begins—from entering a public place to filling a public role.

In the area of the legal protection of this right, Segev attempts to delineate a space of considerations for and against legal protection of privacy in order to enable determination between them and other interests or values (when they exist), especially the right of freedom of expression. He examines considerations such as personal welfare and autonomy, independent thinking, the desire people have for the existence of a private domain and data unexposed to others, socially accepted social practices and conventions, mental health and protection of emotions. On the other hand, he considers factors such as concealing information as insincere and privacy as reflecting social alienation and lack of altruism; diagnoses the distinction between the private domain and the public, general domain as the basis for concealment and suppression of women; and draws our attention to the negative social externalizations resulting from the absence of personal information in decision-making processes. This drawback may harm the quality of the resulting decisions.

The point of departure of **Amit Lavie-Dinur** and **Yuval Karniel**'s article, which deals with the right to privacy in reality TV programs, is that television broadcasts have a double role—that of actor and that of social agent. Reality programs invade the privacy of one person or another but also convey an important social and cultural message regarding the acceptable and proper relationship between private space and public space. Thus, they reflect and shape the changing concepts of privacy. Lavie-Dinur and Karniel identify a trend of change in the concept of privacy in television broadcasts which is manifested not only in the harm done to one individual or another, who is exposed on the broadcasts, but in the deep devaluation of the significance of the value of privacy and its importance. Loss of privacy on reality programs is, in their opinion, an objectification of the person appearing on the show, stripping them of all value and uniqueness, and insulting to them. Moreover, they claim that watching reality shows involving "normal people" as opposed to actors increases the level of identification on the part of viewers, who think that those regular, individual people are like them. Accordingly, when an invasion of the participants' privacy occurs, an invasion of the viewers' privacy, beyond the normative, accepted degree, occurs as well.

Binyamin Shmueli raises another aspect of the right to privacy in his article, clarifying the significance of the separation of private and public, person and space. Shmueli accomplishes this by discussing two cases that reached the court regarding the publication of a photograph of a person that was taken by the media in the public domain. One case concerned the publication of

photographs from the guarded prison of Yigal Amir, murderer of Prime Minister Yitzhak Rabin, following a request for an injunction against a television broadcasting of photos from his cell, by virtue of the claim that a prison cell constitutes an individual's domain, or alternatively, though the cell is considered a public domain, the photos are humiliating and their publication would be inappropriate since their subject is a religious person. The other case is that of an ultra-Orthodox man distributing religious articles at a street stall photographed in front of a provocative poster of an exposed woman, who, after the photo was published in the newspaper, sued for damages for the infringement of his privacy.

Shmueli dwells on article 2 (6) of the Privacy Protection Act (PPA), which views publication for profit as an infringement of privacy and as representative of the inherent tension between protection of privacy and the activity of commercial mass media. Shmueli suggests that the article, emptied of content by the courts in two cases, be replaced by a "dominance" test. Pursuant to this test, the act of displaying a picture or audio-visual presentation by a commercial mode of communication creates an assumption that the purpose of the broadcast is for profit, a civil wrong pursuant to article 2 (6) of the PPA. The burden of proof that the issue is of public interest and refutation of the assumption should fall, according to Shmueli, on the media. Additionally, he suggests adopting a deconstructive approach toward content, examining not only the infringement of privacy but also the public's interest in it, not only according to the "entire article" test, but to parts of articles as well. Therefore, Shmueli is of the opinion that in cases of deliberations regarding requests for injunctions, partial content publication should be made possible, e.g., blacking out the face or blurring the image; this will protect the right to publish material while simultaneously preventing excessive damage to the right to privacy.

The anthology closes with a view to the new media. **Yair Amichai-Hamburger and Oren Perez** argue that the existing legal concept of the right to privacy is incompatible with the digital reality and that the internet has created conflict with regard to the idea of privacy. On the one hand, the beginning of online activity was tied in to the concept of anonymity. Anonymity is identified with the idea of privacy because the inability to identify the user's details prevents surveillance and penetration into his or her own personal zone. On the other hand, the individual's ability to exercise autonomy in cyberspace depends, in many contexts, on relinquishing privacy. In this respect, the principle of respect for the autonomy of the individual actually makes it necessary to employ flexibility in the demarcation of the boundaries of the right

to privacy. Protection of the right to privacy that is overly meticulous can affect an individual's ability to exercise his or her autonomy.

Amichai-Hamburger and Perez indicate a gap between the attempt to define the right of privacy and the right of anonymity in absolute terms and the world of needs and preferences of internet users. They believe that patterns of behavior on the internet indicate that people do not demand or expect that the internet provide them with anonymity and complete privacy, and therefore, an absolute solution that prefers a certain aspect of the conflict out of a hierarchic perception of rights and values (for example, the autonomy of the individual or public order) will harm other interests and values. Additionally, they draw attention to the law's limited ability to respond to the issue of privacy due to technical arguments such as the network's global nature and the inability of the legal system to adapt to changes, and due to substantial arguments centering on the legal system's tendency to use dichotomous outlines to protect rights. This tendency, in the context in question, ignores the fact that cyberspace creates an internal conflict in terms of the value of autonomy: in some aspects, any concession to privacy (and anonymity) during internet use can allow a fuller implementation of the individual's autonomy, whereas in other aspects, realization of autonomy actually requires the protection of privacy by ensuring the anonymity of the user. Moreover, the constitutional concept of the right to privacy—that places the state as a key player in the game of privacy protection, both as one entrusted with fortifying the privacy concept and as its greatest enemy-ignores the considerable weight of private players on the web.

Amichai-Hamburger and Perez do not ignore potential technological solutions, but introduce the difficulties they present, such as the gap between business interests and the interests of users and those of society in general, and the lack of awareness among users (called "cognitive failure") of these solutions.

Amir Fuchs discusses three uses of the internet employed by terror organizations: The first is using the Web as a mode of mass media to spread propaganda and data; the second is instrumental usage for communication between activists and entities in the organization, gathering intelligence and recruiting of activists and funds; and the third is that of direct use, i.e., cyber terrorism. These uses largely overlap the contact the Web has today with all areas of civil, commercial, governmental and military life, and they originate in the structure of the modern terror organization characterized by an inter-state, multi-state character, which is fluid, not

hierarchic (it consists of many cells scattered in different countries) in order to minimize the risk of exposure. These uses pose a real challenge for intelligence services, which are required to deal with websites of terror organizations head on, and in particular, to gather intelligence by intercepting messages sent on the Web and deciphering them.

Fuchs calls to rethink the balance between the right to privacy and security needs, as far as preventing acts of terrorism. Specifically, he calls to reshape the existing wiretapping rules, especially the requirement that each wiretapping order be specific to a particular person or endpoint, referring to a specific phone number or email address. He claims that the current balance is based on the need for a person to listen in on conversations or read correspondences in order to filter through the suspicious material. The rationale behind the existing rules which enable wiretapping specific lines is therefore setting limits for wiretapping by the authorities, so that their extent is not wide enough to cause infringement of privacy.

Efficient content filtering systems that are able to detect suspicious content in accordance with the equations that define such content challenge existing legislation, partly because legislation actually prohibits their operation, but also because they require a change from the traditional paradigm known from the era of telephony. On the internet, Fuchs argues, a new balancing rule can be shaped, one which does not necessarily restrict the law enforcement agencies by end unit (e-mail address), but allows it to utilize other "anchors" according to content or by identifying the user in another way.

In fact, in order to minimize the violation of the right to privacy by using content filtering by "software sniffing," Fuchs suggests stipulating the use of exposure to a small number of people, tighter supervision preventing leakage of information and limiting use to security purposes as opposed to war against "regular" crime. He also emphasizes the necessity of a public debate on the amendment of the Wiretapping Law or legislation dedicated to use in sniffing software.

Another aspect Fuchs refers to is the need to inform the population about the existence of a traffic reading system on the Web. This recommendation may be an appropriate support for forward-looking thinking. As a matter of empirical observation, individuals have less and less control over their personal information. However, paradoxically, we are the principal manufacturers of information about ourselves and we transmit more and more information all the time, voluntarily in fact. The provision of information is presumably done in an attempt to create

contexts that will help us overcome the amount of information that floods us from every direction. Admittedly, public and private bodies alike rely on the assumption that we do not exert control over our own information or that we are unaware of the amount of information concerning us that is held by others.

However, we do not dispense all the information about ourselves on the Web consciously and therefore willingly. Many people are unaware that their every action online leaves behind digital footprints, a "breadcrumb trail" or "digital trail." They believe that their intimate relationship is with "the machine," i.e., with a closed, private network. Therefore, their willingness to share information without objection is increased. It may be said that asymmetry of awareness is the key issue. While large companies and governments accumulate vast amounts of information, the public, the source this information was mined from, is not informed and does not understand where this information is located, and why it is there. This asymmetry is a source of injustice, and even more so—of justified anxiety among individuals.

A clear policy that promotes the level of control of individuals over personal information related to them is imperative, while ensuring that "information holders" inform their "information objects" regarding the information they hold. In an ideal situation, such a policy would be made on an international basis while maintaining four rules: (1) a promise that the citizen be able to freely access information he or she is an object of; (2) reducing the number of exceptions based on national security; (3) expanding the obligations and rules applicable to entities holding private information to private entities and companies as well; (4) the operation of international mechanisms for monitoring and dispute resolution. It is possible that, as far as data mining by private companies, self-regulation that promotes transparency and involvement of users in designing their personal profile could be used as a supplemental method. Forerunners in this regard are the initiative of the Digital Advertising Coalition that offers an "advertising icon"—a logo that shows that the site collects data and enables one to decline data mining with a click.[13]

An essential supplemental method for any regulatory involvement is the promotion of digital literacy among Web users, and in fact, among the general population of the twenty-first century. This refers to the development of acquired skills—technical and cognitive—that promote the individual's relationship with digital space. Participation literacy in the information

[13] http://www.evidon.com/privacy_center.html#forward_i

age is the bundle of skills relating to the actual awareness of one's ability to demand information; understanding how information is collected, integrated, stored, and represented by government and commercial corporations, and the ability to claim control of and involvement in all of the above. Specifically, this refers to the idea that even if a person is at home in digital space, this does not necessarily mean that every aspect of his or her life should be like an e-book, open to the public, providing everyone with access to what he or she says, does, types, messages, photographs, tweets, updates, buys, sells, borrows, steals, eats, drinks, wears, where he or she is and with whom. This is about understanding that every activity in cyberspace leaves a digital trail, which can be used for both positive and negative purposes alike; awareness of the possibility of not agreeing to every window asking the user whether they want the information to be available for the application that they want to download; the need for strong passwords to protect smart computers and cellular phones; implementing the concept that free usage of various platforms does not make the user a client. Instead, the literate user understands that they themselves are the product. It is possible that the most pressing need is to ensure that elected officials are not digital ignorants—that their digital knowledge is of a sufficient level to enable them to stand at the helm of dealing with the challenges to which Western society is called upon to deal with.

Thanks to Professor Mordechai Kremnitzer, who accompanied the collection from its early stages, to the authors of the articles who contributed of their time and talent, and to the dedicated text editors and personnel of the Israel Democracy Institute Press.

Jerusalem, July 2012