PRIVACY PROTECTION BILL

2019-5779

Rachel Aridor-Hershkovitz
Tehilla Shwartz Altshuler

Summary

November 2019

THE ISRAEL DEMOCRACY INSTITUTE

THE ISRAEL
DEMOCRACY
INSTITUTE

PRIVACY PROTECTION BILL, 2019-5779

Summary

Rachel Aridor Hershkovitz | Tehilla Shwartz Altshuler

November 2019

Text Editor [Hebrew]: Anat Bernstein
Translated by Lenn Schramm
Series and Cover Design: Studio Tamar Bar Dayan
Typesetting: Nadav Shtechman Polischuk
Printed by Graphos Print, Jerusalem

ISBN: 978-965-519-265-0

The Israel Democracy Institute
4 Pinsker St., P.O.B. 4702, Jerusalem 9104602
Tel: (972)-2-5300-888
Website: en.idi.org.il

To order books:
Online Book Store: en.idi.org.il/publications
E-mail: orders@idi.org.il
Tel: (972)-2-5300-800; Fax: (972)-2-5300-867

All IDI publications may be downloaded for free, in full or in part, from our website.

I.
Introduction

During the past decade and a half, rapid technological development has created tension and a mismatch between the right to privacy and the practices of collecting, pooling, and processing personal information that are the basis of the digital economy. New and inexpensive techniques for storing vast amounts of personal information; the hyperconnectivity revolution that applies not only to messages and content but in fact to just about everything (from smart devices to nano-bots inside the human body itself), which enables the continuous transfer of Big Data from sensors and devices that gather personal information to central "brains"; and the artificial intelligence revolution, which permits analysis of data, including the personal information that has been amassed: all of these have expanded dramatically.

As a result, states and giant corporations are becoming "personal data miners." We can say—to borrow a term from the European Union's directive on data protection—that we are all in practice "data subjects." The heart of the digital economy and the business model of the behemoths (Google, Amazon, Facebook, and others) are based on the collection of increasing amounts of personal information and its analysis to produce new insights. In addition to the giant corporations, millions of small and medium businesses are constantly aggregating personal information. Databases of personal information, ranging from individuals' internet use patterns to their medical history, are of immense economic value. Governments are not lagging behind and have developed systems to collect various categories of personal information—whether received as a result of their routine activities (such as education, taxation, healthcare, and welfare services), produced by video surveillance in public places, along with heat and sound sensors to identify citizens and monitor their

activity, and amassed from databases of biometric data or through active data collection from the social media.

The intensive collection of personal information and the inherent advantages offered by technology require new thinking about the right to privacy and the current Israeli regulations under the Privacy Protection Law, 5741-1981. The coming into force of the EU's General Data Protection Regulations (hereinafter, GDPR) in May 2018,[1] and the exposure of problematic uses of the personal information of millions of users throughout the world, including Israeli citizens (as in the Cambridge Analytica scandal), strengthen the view that Israel is in desperate need of a new privacy protection law.

The Privacy Protection Law was passed in 1981 and has been amended several times. Chapter 4, on imparting of information or data items by public bodies, was added in 1985, Chapter 2 on data protection was updated in 1996; amendments in 2007 altered the definition of "consent" and provided for the payment of damages in certain circumstances, even without demonstration of harm.

Since the start of the current century, there has been general recognition that the law's provisions need to be re-examined and a set of amendments formulated. The main reasons for this are the entrenchment of the right to privacy as a constitutional right in Section 7 of the Basic Law: Human Dignity and Freedom, and the technological innovations that have led to the increasing use of computerized databases in new ways that were unknown when the law was passed. The amendments to date have been extremely minimal, leaving a lacuna in the protection of privacy in Israel.

Furthermore, in 2011 the European Commission recognized Israeli law as compatible with the EU's privacy protection regime and the adequacy of its personal information protection. Because Europe is Israel's main

1 The General Data Protection Regulation 2016/679.

export market, this recognition allows the simple and easy transfer of data between the EU and companies, organizations, and research institutes in Israel. However, this recognition is currently being reconsidered, and may be withdrawn because of the growing disparity between the GDPR and the out-of-date Israeli Privacy Protection Law and the provisions added to it since 2011. In this sense, there is a unique convergence of interests in revamping the law, among Israeli civil society and human rights organizations, the private sector—led by the "start-up nation" technology sector—and academic and research institutions.

In May 2016, 35 years after the Privacy Protection Law was enacted, we launched a joint project with Adv. Haim Ravia, head of the cyber law group at Pearl Cohen Zedek Latzer Baratz, to develop a new version of the law. We convened a group of experts, comprising attorneys, academics, and technology experts; from the public service, civil society, the private sector, and industry, with the aim of formulating a proposal for a new privacy protection law that would satisfy today's needs—including a definition of the right to privacy, the protections offered by the law, and its suitability to the digital world.

The path we took was not marked out in advance. Every question was put on the table. For example, is it appropriate to combine a statute on classic privacy protection with a data privacy law? What should and what should not be taken from the GDPR, and what might it be better to borrow from the laws of other countries, such as Australia, Canada, and New Zealand? How should the provisions of the GDPR be adapted to suit the specific circumstances of Israel and its residents, but so that they still function in a world of cross-border transfers of personal information? What shortcomings are already becoming evident in the GDPR and should accordingly be avoided? What judicial approaches to the scope of the right to privacy have developed in Israel over the years and which aspects of them are worth maintaining? How should we relate to pending legislation, such as Amendment 13 to the Privacy Protection Law? What

technological challenges confront us: for example, can the "right to be forgotten" exist in a world where learning machines never forget any of the data they were trained on?

The heterogeneous structure of the group required us to address different ideas about the complex balance between the protection of basic human rights, which some of us saw as "the ultimate human right in the digital world" in that it is tied to the essence of the digital economy and the fears of the emergence of a "surveillance society," on the one hand, and industry's ability to innovate and pursue technological and economic development while subject to restrictions, along with concern about the possible harm to small firms that cannot satisfy privacy protection requirements or cope with disproportionate regulatory burdens.

We believe that the current Privacy Protection Law should be repealed and replaced by our proposed text, which we refer to here as the Privacy Protection Bill. We also propose stipulating that the new law take effect one year after its passage. We believe this interim period is sufficient for making the changes it would mandate, primarily in light of its great compatibility with the GDPR. Corporations and organizations that already comply with the GDPR for various reasons would not be required to introduce major changes in their current privacy protection policy.

The bill is a contribution to Israeli society and the State of Israel. A serious discussion of the right to privacy, along with a clear definition of the rules of the game and the required ancillary arrangements, in the various contexts in which it affects our lives, is the need of the hour. We hope that decision-makers will make use of our proposal for the benefit of all Israelis.

II. The Need for a New Constitutional Theory of the Right to Privacy

Before we address the novelty of our bill, we should note the constitutional approach on which it is based. The intensive collection of data and the advantages offered by technology have spawned the cynical idea that privacy is dead. Not only do we believe that this idea is wrong; we think it imperative to create a relevant constitutional theory for the protection of privacy, both to justify this protection and to serve as a theoretical framework for interpreting the law in the future. The constitutional theory we offer is based on three main pillars, which we will review now, and which later receive expression in the bill's Purpose Articlel.

1. Privacy as Control

The natural response to the broad-scale collection of private data in recent decades has been an increased perception of the right to privacy as individuals' control of information about themselves. This approach is based on the fact that every person has the ability to decide which parts and areas of the private sphere he or she allows others to access, and the ability to control the degree, scale, and timing of their exposure. Thus, unlike other human rights, and in a more extreme fashion, the right to privacy is a one whose boundaries allow compromise and concessions. The information is mine, and I am the only one who can decide what happens to it: I decide on its economic value for me and what I gain or lose if I surrender it. If I want, I can sell it; if I want, I can change my mind and demand that what I have provided be expunged. It is my right—thanks to this control—to view the databases that contain information about me; and it is certainly unlawful for others to make use of this information

without my consent, other than in exceptional cases. I have the privilege of approving the terms of service before I download an application or start using free programs whose entire business model rests on using my data.

The "privacy as control" approach has become standard in Europe in all matters related to the analysis of privacy disputes. It is central to the GDPR and expressed in the substantial formulation, fine-tuning, and expansion of the set of data subject's rights: the right to inspect the information; the right to delete it, correct it, or transfer it to another company; the obligation to notify data subjects what is done with their data; and a better awareness that the waiver of data privacy is the basis for providing consent to collect and process data. This is also the dominant approach in Israeli legislation and constitutional thought. In the Basic Law: Human Dignity and Freedom, the right to privacy is enumerated alongside the right to property, rather than with other civil and political rights such as freedom of expression and freedom of religion, which are not anchored in law, and refers to the prohibition on entering an individual private domain without consent. Article 1 of the Privacy Protection Law states the framework for privacy protection in Israel: "No person shall infringe the privacy of another without his consent."

The "privacy as control" approach is also widespread in the academic literature, where there are many studies that address the question of informed consent for the waiver of privacy, when it is required, and when it can be assumed that there is a reasonable expectation of the protection of privacy, such that its infringement requires consent, and the like.

Although this approach is important, we do not believe that it can stand as the sole basis for protecting privacy in the twenty-first century. This is because limiting privacy to the notification and consent mechanism has led to the creation of fictitious aspects, to the point that the request for consent is one of the most common ways of laundering violations of the right to privacy in this generation.

First, it is difficult to consent to a breach of one's privacy in a world where information is processed in a variety of ways and for diverse goals, some of which could not have been anticipated when the consent was given. A major advantage of learning machines is their ability to identify unexpected ideas and patterns. For example, consent to the installation of surveillance cameras in preschools, in order to safeguard the children, could lead, in a world of major advances in video-analytics, to the possibility of producing a social ranking of young children by their abilities, their potential for success in their future schools, and the like, and serve as the basis for their classification at a very early stage of life. It is doubtful whether all parents are aware of this when they consent to the placement of a camera in their children's preschools. In addition, it is generally assumed that information that has been anonymized can be published and processed with explicit permission. However, recent studies indicate that the capacity to de-anonymize data is improving; here too the difficulty in predicting technological advances has repercussion for the need to require data subjects' consent for such processing.

Second, the psychological phenomenon of the "privacy paradox" reflects an essential mismatch between the privacy approach as expressed by users ("I care a lot about my privacy") and their actual behavior (providing information in return for monetary or in-kind benefits). Most of us do not use web browsers that enable greater anonymity; we are willing to provide information in order to benefit from services, to use social networks, to receive a birthday present in exchange for using a club card, and to use location-based services. Moreover, most of us do not read terms of service, even when they are relatively short or written in large letters. It is possible that this is even rational behavior, which expresses optimism (nothing is going to happen) or reliance on others (if there is a problem, someone will file a class-action lawsuit and we will share in the award). Third, consent to provide personal information can also have negative externalities that affect other people. If our joining a social network allows the platform

to access our contact list, and tagging faces makes it possible to know who was with us in photos we uploaded, even if those third parties are not active on the platform, and if providing genetic information makes it possible to learn a great deal about family members (sometimes even fingering them for criminal activity and sending them to prison for many years)—clearly my consent about my information affects others as well.

In summary, the drawback of the "privacy as control" approach is primarily that our control of our personal information is largely imaginary; this is effectively the major privacy crisis of our generation. Beyond the need to augment the public's digital literacy, a task that is important but of limited effectiveness and would take a long time, the corollary of such a constitutional approach is that consent is no longer seen as the exclusive means for commerce in data-control rights. In other words, it is necessary to determine standards for the legitimate and reasonable use of personal information and to require companies to request the consent of data subjects only in the case of illegitimate uses. The transfer of responsibility from users, with whom it currently rests because of the requirement for consent, to those who process the data—who will have to justify the uses they make of the data—is the best way to address the right to privacy today.

We followed this logic when we drafted our bill, by defining, as the European legislation does, "legitimate grounds" for the infringement of privacy—of which consent is one, but not the sole basis; and when we defined an absolute right to withdraw consent, as a way to create an incentive for those who process data to request consent only as a last resort.

2. The Right to be Left Alone

The second constitutional pillar of the right to privacy in the digital world relates, somewhat paradoxically, to the basic and classic meaning

of the right to privacy—what is called "the right to be left alone." This is the right of all individuals to preserve and protect their identities and a protected space around their bodies, thoughts, emotions, confidential secrets, lifestyle, and intimate activities. Privacy, in this context, is seen as an essential element of the ability to maintain one's identity and to develop relations of love, intimacy, and trust with those around us, and of the ability to fulfill the psychological need to be alone, with the goal of endowing us with emotional tranquility in the knowledge that there are places where no one else is with us. This is in practice the classic approach to privacy, which is at the core of disputes that involve the unlawfulness of entering people's homes, intercepting their private conversations, photographing or recording them without their consent, and so on.

In a world where we are surrounded by sensors, cameras, recording devices, and other instruments that constantly monitor our activity—from nano-bots inside the circulatory system (tiny devices to monitor health indices in the blood stream), to smart beds and intelligent personal assistants—we are never alone. This has far-reaching psychological consequences. If in the past the digital world could make us envy our friends' stunning pictures on Twitter, feel depressed because of our overuse of Facebook, enslave us to addictive applications and devices, and even produce the phenomenon of "online disinhibition"—meaning a willingness to input messages we would never consider saying face to face, which leads to shaming and harassment (from social exclusion among young people to "revenge porn" among those who are older)—now, in a digital world where privacy is non-existent, we can anticipate substantial emotional costs, such as the development of a human-like relationship with devices and dependence on devices; psychological arousal, agitation, and anxiety because we are always being seen; and the like.

One feature of intelligent personal assistants ("self-restraint preference algorithms") such as Amazon's Alexa, Google Home, Google Duplex, Microsoft's Cortana, and Apple's Siri—end-user products based on

artificial intelligence that have already made major market penetration and that are intended to accompany us wherever we go, whether on our cellphone or as a constant presence in the home or workplace—is the human attributes (voice, face, language) with which they are endowed by their developers. The presence of these devices is supposed to give us the feeling that there is another person with us, that someone is listening to us, conversing with us, or watching us. In contrast with our behavior towards what we think of as a "machine" (such as a computer or telephone), studies show that we respond to anthropomorphized technology as if it were a real person. For example, people who see a machine that communicates with them in a human manner develop a closeness and trust with it and are willing to answer sensitive personal questions or provide personal details they would not have been willing to give to what they see as a "mere machine."

Such interfaces have major advantages, including alleviating the burden of solitude for those who suffer from it. But the fact that we are accompanied at all times and in all places by what we intuit as a human being (although it is not) can have severe ramifications for our emotional state. Today we are placing machines in places where we would never admit human beings; and by doing so—given that we know that these machines indeed track us and monitor our activity—we are introducing a "spectator" into extremely intimate situations. This can produce constant emotional stimulation because of the sense that our actions are always being monitored. Ultimately, this would seem to be the reason that the right to be left alone emerged in the first place, albeit in different circumstances.

In addition, from the constitutional perspective, there is a need for proportionality tests that ask frankly whether there is a true commercial, economic, or public need for this obsessive collection of private data about us. Against the undoubted advantages for technological progress, commercial convenience, or even law enforcement, we must weigh the

chilling effect of the knowledge that they are constantly being monitored—always, in every place, and in all situations—on people's curiosity, their trust in others, their intimate activities, and also, and no less important, on their creativity and ability to think outside the box, which are the most important germs of innovation. It is no surprise that in countries where there is no freedom and there is constant monitoring, like China, there is also no inherent innovation and new ideas must be procured from other countries. In this sense Israel is at the opposite extreme. It is easy to say that it is precisely in a small economy that innovation should receive priority over privacy. In our view, however, we cannot preserve innovation without providing every person with a safe private space.

It is in this light that we drafted the Purpose Article of the bill, in which we wrote: "The purpose of this bill is to protect a person's privacy *in order to ensure the autonomy of the individual, including the protection of his/her personal space, the privacy of his/her personal life, the confidentiality of his/her communications …"*

3. Privacy as a Precondition for a Sound Democratic Process

The third constitutional pillar of the right to privacy is the idea that privacy is a precondition for blocking the ability of various entities to aggregate personal information with big data about others in order to create extremely precise personality, psychological, and behavioral profiles through analysis based on machine learning.

In a world where it is possible to pool and analyze information about us in order to generate buying and behavior recommendations "just for you" (purchases on Amazon, shows on Netflix, navigation guides such as Waze), we are consciously surrendering some of our decision-making freedom to systems that know what is the best route to our destination and what we should eat; we are also exposed to attempts at individual persuasion

tailored to our measure, with a power, invasiveness, and effectiveness that did not exist in the past.

The intelligent personal assistant systems mentioned above, which are designed to learn as much as possible about us—our interests, purchases, health, friends, habits, mood—and then help us send messages, make phone calls, set appointments, order products, and make travel reservations, are supposed to provide us efficient and useful proactive recommendations precisely when and where we need them.

But suppose our digital assistant reads an email from our doctor that the results of our last blood tests were worrisome, so we need to lose weight and avoid certain foods. And if our wearable computer informs the intelligent assistant that we aren't exercising enough or have gained weight? And if the assistant knows that every Friday we buy three cream cakes at the bakery? What should it do? Delicately suggest that we skip the cake this week? Display a graphic warning, like that on cigarette packs, about the harm caused by obesity? Threaten that if we keep buying cake it will block our access to Candy Crush (and even make good on the threat)? Send a message to the doctor, behind our back, to tell her about our cake-buying habit? Instruct the credit-card company to block our purchases from the bakery?

And what if the bakery works with the same company? Or our health insurance provider, which wants to keep us from buying unwholesome foods so it won't have to pay for treating our medical problems in the future? In short, should the intelligent assistant be able to use our private data to prevent us from making decisions that are bad for us? Or should it help us satisfy every immediate wish and appetite, and the consequences be damned?

This phenomenon, which we call the "autonomy trap," is essentially the realization that a key concern related to privacy is not just the collection of information, but also the potential applications of data processing.

We know that users' behavior on social networks can be employed to extract knowledge about their emotional tendencies, insecurities, fears and anxieties, sexual orientation, and more. Similarly, recordings from surveillance cameras can yield insights into behavioral deviations and interpersonal capabilities.

The problem is that a personality profile can be used for retargeting advertisements to purchase products or services or for other forms of influencing behavior—all of it in a way that is precisely tailored to the needs associated with the profile. Of no less concern, we must remember that it is only a stone's throw from the use of techniques for collecting personal information in order to suggest products and services to the application of the very same techniques to influence our thoughts, create an autonomy trap about beliefs, undermine our trust in democratic institutions—in brief, to manipulate elections.

The Cambridge Analytica scandal in the spring of 2018—which took the lid off the exploitation of personal information to tilt elections in many countries—shows that the right to privacy goes far beyond individual control of information and in fact involves a threat to the very possibility of conducting a sound democratic process and thus of protecting all human rights. So even though the existence of perfect and convincing artificial intelligence systems has not yet been demonstrated—systems that can identify people who are vulnerable to efforts to alter their opinions, design individual and invasive tools specifically for those people, and create behavioral and emotional profiles for use in election campaigns—such systems are today's hot story.

On the level of constitutional theory, then, we must realize that the right to privacy can no longer be only the atomistic right of every individual to control personal information; it must now be viewed as including collective aspects as well. Without privacy there cannot be a sound democratic process based on free choice. This means that defense of

the democratic system, as a collective interest, is intrinsically linked to the right to privacy. On the conceptual level, the right to privacy must experience the same developmental process that its older sibling—the right to freedom of expression—has traversed. Just as the right to freedom of expression evolved from each individual's right to shout aloud whatever comes to mind into the collective right to maintain the diverse and functional public discourse required for a sound proper democratic process, so too privacy must evolve from every individual's right to control personal information to the collective right to protection against autonomy traps that manipulate elections and minds. Without privacy there is no meaning to an individual's life; and without privacy there is no meaning to democracy.

This is why the Purpose Article of our bill states as follows: "The purpose of this law is to protect people's privacy, *to enable individual autonomy ..., to safeguard a sound democratic process, and to prevent unfair influence based on the processing of personal information about an individual.*"

III. The New Features in the Bill

1. Integrating Classic Privacy Protection with Data Protection

Before delving into the novelty of the bill, it is important to note that, after long hesitation, we decided that our text should retain the integration of classic privacy protection with data protection. We did so even though in most countries, including the EU, privacy protection laws focus on data protection. We were guided by the desire to retain the existing statutory structure in Israel, so as to avoid problems with the assimilation of the new law by the legal system, the public sector, and industry; by the fear

that the legislative process would be slowed if two separate bills were proposed; and by the aspiration to produce comprehensive and innovative legislation that protects every conceivable form of privacy.

2. The Purpose Article

The decision to attach a Purpose Article to the bill was meant to assist in the judicial interpretation of the text and to make it clear that the purpose of protecting the right to privacy comprises three elements: First, protecting the right to be left alone, the confidentiality of communications, and the confidentiality of private personal life—the germ from which the classic right to privacy developed. Second, protecting individuals' ability to control personal information about themselves that is collected or processed by others, as part of the core activity of the digital world and the data-based economy. Third, protecting people's ability to make decisions in a free and autonomous manner, especially with regard to democratic elections, in a world where the processing of personal information can generate "autonomy traps" and lead to targeted invasive attempts at persuasion of a sort unprecedented in human history. These three elements are intended to produce an ethical and technologically neutral framework for protecting privacy in Israel in the years to come.

3. Definition of the Infringement of Privacy

The current Privacy Protection Law defines a closed list of infringements of privacy, with no logical or theoretical links among them. In addition, the current law does not cover forms of infringement that may take place in the course of digital data-processing. We accordingly updated the closed list of categories of infringements of privacy found in the current law. To the list of classic violations (such as harassment, photography in the private domain, publication of private information with the potential to humiliate or shame, eavesdropping and wiretapping, unauthorized use of a person's name, violation of the confidentiality provision defined

by law) we added two new categories: viewing or examining personal information; and processing an individual's personal information in violation of the statutory provisions. These categories will be the backbone for the protection of the privacy of personal digital information.

4. Elimination of the Obligation to Register Databases

The obligation to register databases is one of the anchors of the current Privacy Protection Law. This requirement became a dead letter because of a lack of adequate enforcement, because it does not ensure the protection of privacy, and because of the abolition of the registration fees by the Privacy Protection Authority as of August 2017. In addition, we believe that in the digital world, where personal information is gathered and saved on a routine basis, this requirement places an unreasonable regulatory burden on almost anyone who maintains a list of customers, consumers, or users of a service they offer. We believe that the alternative set of tools for data protection that we propose (see details below) will provide a more precise and comprehensive solution for protecting privacy than has been offered by the requirement to register database.

5. Technological Neutrality

We propose formulating the provisions in terms that are as general and technology-neutral as possible. This is why we chose, for example, to remove Chapter 2, Part 2 of the Privacy Protection Law, which deals with direct mailings.

6. Definitions

We refined the definitions found in the current Privacy Protection Law, including the following:

(**a**) We replaced the terms "Manager of Database" and "Possessor of Database" with Controller" and "Processor," in keeping with the deletion of the reference to the database registration requirement and to coincide with the terminology of the GDPR.

(**b**) We replaced the definition of "Information" in the current Privacy Protection Law with a more precise category of "Personal Information." The new definition is broader and covers "data about a person who is identified or can be identified with reasonable effort," rather than listing various types of information, such as that about a person's personal status or health.

(**c**) We expanded the definition of "Sensitive Information" in the current law so as to include information such as ethnic origins, criminal record, biometric data, and genetic data.

(**d**) We replaced the current law's reference to the "use" of personal information with the "Processing" of personal information. Our proposal defines a closed list of three forms of activity: collection, analysis, and distribution. As such it is appropriate for the full set of activities that can be performed with personal information in the digital world.

(**e**) We defined "Consent" as that which is provided knowingly, explicitly or implicitly, as in the current Privacy Protection Law, and added that the requirement that consent be granted "freely." The change we propose expresses the need for data subjects to have better control of their personal information, in a formulation based on that in the GDPR.

7. A Change in the Concept of Consent

The natural legislative response to the massive gathering of personal information about many aspects of our lives is to upgrade the right to privacy to give individuals better control of information about themselves. The first corollary of such control is the ban on using personal information

without the consent of the data subject. This is the standard approach in many countries, including Israel, for the analysis of privacy conflicts, and has a very important place in the GDPR. The downside of this approach is that excessive dependence on the requirement of consent, in a world in which personal information is processed in various ways and for purposes that could not be foreseen when the consent was granted, is problematic. Moreover, scholars of behavioral economics have found that people tend to grant consent as a matter of course. There is a disparity between people's attitude towards privacy as expressed by their own statements and their actual conduct. Behavioral economists also assert that one person's consent to an infringement of privacy can have negative ramifications for others. For example, when individuals join a social network, the network may be given access to their contact list; tagging people's faces in pictures enables networks to learn about other people in the picture ("tell me who your friends are and I'll tell you who you are"); and a person's consent to provide genetic information to a data processor can lead to information about his or her relatives.

We believe that the solution to this problem is for a clear statutory definition of when it is legitimate and reasonable to infringe a person's privacy. We also propose seeing consent as an important means, but not the sole or even the primary means, for allowing infringements of privacy. In our proposal, an infringement of privacy is any action that does not comply with the provisions of the law; this replaces the stipulation in the current text Article 1 of the Privacy Protection Law that "no person shall infringe the privacy of another without his consent." Our proposal enumerates legitimate grounds for breaches of privacy, including by the processing of personal information and sensitive information; only the last of these grounds, in order of appearance and importance, is the data subject's consent. We also stipulated that the data subject has the right to withdraw that consent and that the Controller must take this possibility into account.

8. The Processing of Personal Information about Minors

Based on a proposal by the Israel Internet Association (R.A.) regarding the use of the personal information of minors below the age of 13, we added the obligation to receive consent from a parent or guardian before infringing the privacy of minors, including the processing of their personal information.[2] We also proposed that the Privacy Protection Authority set guidelines for verifying minors' ages and for modes of consent, and that in the case of an infringement of privacy through the processing of sensitive data, parental consent be required for minors under 16.

9. The Requirement of Fulfilling the Purpose

We expanded the principle stated in Section 9(2) of the current law ("The Principle of Adhering to the Purpose"), which stipulates that information may not be used for purposes other than that for which it was collected, and added a separate clause, in affirmative language (based on a similar provision in the GDPR), that it is permissible to process personal information for a purpose similar to that for which it was initially collected. The reason for this stipulation is that it is not always possible to foresee with precision the scope of the purposes of processing personal information that has been collected. We also understand the personal information-processing industry's need for room to adapt to new developments and for innovation.

2 Privacy Protection Bill (Amendment—Protecting the Privacy of Minors), 5777–2017.

10. Strengthening the Right to Control Personal Information

The bill includes a list of rights that do not exist in an identical format the current law and that are aimed at strengthening data subjects' control of their personal information.

These rights are as follows:

(**a**) Expansion of the *right to inspect personal information* so that it includes, in addition to data subjects' right to view their personal information itself, the right to know the source of the personal information if it was not collected from the data subjects directly, the purpose for which the personal information are being processed, and to whom the information is conveyed. However, our text permits denial of requests to inspect personal information not only in cases of concern about potential harm to physical or mental health, but also in cases of endangerment of human life or a serious violation of the rights of a third party.

(**b**) Addition of *the right to receive an explanation* when personal information is processed mainly by automatic means, and when a decision taken in the wake of the processing of personal information has a significant impact on some statutory right or duty of the data subject—in order to permit a review of decision-making processes by machines and further study of any biases they may involve.

(**c**) Addition of *the right to data portability,* which, as an essentially economic right, entails the ability to transfer data sets that include personal information to other data processing platforms without the need to invest resources or new effort.

(**d**) Addition of *the right to be forgotten,* which is in practice the right to delete data, and which entails data subjects' ability to demand the deletion of data if they withdraw their consent, or if it emerges that the

processing was performed for purposes other than those for which the information was collected, or in violation of the law.

(**e**) Expansion of *the obligation to notify* data subjects of their rights, with details of the topics that must be included in the notice, the extent to which the processing is requisite for achieving the goal, and the contact details of the party that wishes to process the data.

11. Expanding the Obligations of Controllers and Processors, as Relevant

We expanded the obligations of controllers or processors, as relevant, to safeguard the confidentiality of the personal information they are processing and to secure the personal information they control or process.

These obligations include, among others:

(**a**) The provisions of the Privacy Protection (data security) regulations, 5777-2017, which came into force in May 2018, were incorporated into the primary legislation as an ethical statement that recognizes the importance of protecting personal information in the digital world. However, we did not adopt the model found there, which distinguishes medium and high levels of data security as a function of the number of data subjects in a database. In the future we will propose an amendment to the data security regulations that is compatible with what we propose in this bill. For now, so that we can present a full picture of all the proposed amendments, we chose to include the amendments in the bill.

(**b**) Provisions for data security in the spirit of the new data security regulations, the amendment to the Australian Privacy Protection Act, and the GDPR, which include *the obligation to document and report security-related events*; the obligation to prepare a survey of the impact on privacy in cases we defined; and the appointment of a privacy protection officer by companies that process personal information.

(**c**) *Privacy by Design:* The obligations of the controller are augmented by the obligation to include data privacy measures starting in the planning and development stags of systems for processing personal information, and afterwards in the stages of their dissemination and implementation—through the adoption of the requirement of "privacy by default" and "privacy by design," similar to the stipulations of the GDPR.

12. Extra-Territorial Application

In a digital world where multinational corporations process the personal information of data subjects located in Israel, and corporations located in Israel process the data of persons located outside Israel, it is crucial to define extra-territorial arrangements for the protection of privacy. We added a clause stipulating that the law applies to any entity incorporated or operating in Israel that processes personal information. These provisions also apply to the processing of the personal information of data subjects located in Israel by corporations located outside Israel, similar to the stipulations of the GDPR.

13. Strengthening the Privacy Protection Authority

On the institutional level, our proposal strengthens the Privacy Protection Authority and turns it into an independent investigative and enforcement agency, responsible for its own budget and hiring, like the Antitrust Authority and the Consumer Protection and Fair Trade Authority.

(**a**) We defined a clear list of *positions within the Authority*, similar to the stipulations of the Consumer Protection Law.

(**b**) Incorporating the arrangements of the proposed Amendment 13 to the Privacy Protection Law, submitted to the 20th Knesset, the bill includes the *administrative enforcement powers* defined there. However, rather than taking over the text of the proposed Amendment 13 word for word, we

modified its provisions to coincide with our bill and with the provisions for administrative enforcement powers defined in the Consumer Protection Law 5781–1981. These provisions represent the current statutory framework on this topic, and we believe it is important to maintain consistency in legislation that grants administrative enforcement powers to a public authority.

(**c**) Our proposal expands the investigative powers of the Privacy Protection Authority to include *associated offenses*, similar to the powers currently invested in the Antitrust Authority.

(**d**) We defined provisions *for cooperation with foreign agencies* for the purpose of investigation and enforcement, similar to the provisions of the Securities Law 1968, based on a recognition that, in light of the international and global character of personal information processing, such cooperation will be crucial for enforcing protection of the right to privacy.

(**e**) We proposed *disbanding the public council* established by the current law, which in practice lacks any operative powers, and replacing it with an advisory committee to the Privacy Protection Authority, similar to that created by the Consumer Protection Law.

(**f**) We proposed adding the *right to appeal* any decision by the Privacy Protection Authority to the Administrative Affairs Court.

14. Refining the Law's Implications for Damages and Criminal Offenses

Our proposal stipulates that tort and criminal liability will apply only for the violation of specific provisions in the law.

(**a**) The current law imposes tort liability only in the case of an infringement of privacy. We propose extending it to the provisions that relate to an

infringement of privacy, to the duty of notification, and to all of the data subjects' rights and their mode of implementation.

(**b**) Criminal liability will be incurred by any violation of Article 4 (Infringement of Privacy). Because we defined the infringement of privacy in a more precise and logical manner than the list found in Article 2 of the current law, there was no need to exempt some of its subclauses from criminal liability.

(**c**) We provide for harsher criminal and tort sanctions in a case where minors, the elderly, or the helpless were the actual or intended victims of the offense.

(**d**) We have added *criteria* for setting the amount of compensation.

15. Recognized Defenses

(**a**) We stipulated that the recognized defenses will apply *in every legal or disciplinary proceeding,* and not only in criminal or civil proceedings, in order to permit coherent interpretation of the legislation.

(**b**) We added the defense that processing of the data is required *to fulfill legal obligations.*

(**c**) We retained the defenses of publication pursuant to the Prohibition of Defamation Law and of *good faith and the public interest,* in order to protect investigative journalism so that it can do its job properly and the publication of information that is newsworthy and of public value.

16. Abolition of the Blanket Exemption from Liability for Infringements of Privacy by the Defense and Security Services

The increasing use of technology for surveillance, law enforcement, and the war on crime, through the integrated analysis of personal

information and big data, has augmented the risk of flagrant and widespread infringement of the right to privacy by security and law-enforcement agencies. Accordingly we deemed it inappropriate to retain the section that permits the infringement of privacy by a security agency in accordance with the criterion defined in Article 19(b) of the current Privacy Protection Law—the test of reasonableness—as long as the breach of privacy took place as part of and in fulfillment of the agency's assigned mission. Moreover, in the years since Article 19(b) was enacted in 1981, the right to privacy has been anchored as a core constitutional right in the Basic Law: Human Dignity and Freedom. Accordingly, we believe that the law should not permit infringements of the right to privacy that do not meet the requirements of the "Violation of Rights" clause (§8) in that law. Moreover, the delegation to security agencies of blanket authority to conduct surveillance and infringe privacy could become an obstacle to European recognition of the adequacy of the Israeli privacy protection law for protecting privacy. Hence our bill would eliminate the current exemption enjoyed by the security services. At this stage we chose not to define a comprehensive arrangement and have instead proposed the passage of a specific law on the subject that would grant explicit and proportionate authorization. That law would address the use of technologies that infringe privacy for the purposes of law enforcement, surveillance, and crime prevention.

Attorney Rachel Aridor-Hershkovitz is a researcher in the Democracy in the Information Age Program of the Center for Democratic Values and Institutions at the Israel Democracy Institute. The holder of LL.B and LL.M degrees, her Ph.D. dissertation at the University of Haifa deals with frameworks for cooperation between government and industry to increase protection of cyberspace.

Dr. Tehilla Shwartz Altshuler is a senior fellow at the Israel Democracy Institute and head of the Institute's Media Reform and Democracy in the Information Age programs. She is a senior research fellow at the Federmann Cyber Security Center at the Hebrew University of Jerusalem. She is also a board member at the Israel National Press Council. She is an expert on media regulation and the interface between technology, law, and policy.

www.idi.org.il

THE ISRAEL DEMOCRACY INSTITUTE