

# **Research Article**

## THE FUNDAMENTAL CHALLENGES FOR PROTECTING PERSONAL PRIVACY IN THE AGE OF THE NETWORK

### \*Dr. Yair Oppenheim

Tel Aviv University, The Lester and Sally Antin Faculty of Humanities, School of Philosophy, Linguistics and Science Studies

#### Received 20th March 2025; Accepted 18th April 2025; Published online 30th May 2025

#### Abstract

Personal privacy, in its various aspects, has occupied human beings since the dawn of mankind. The concept of personal privacy has developed and varied throughout human history. In the last two decades, the privacy issue has never left the public agenda. Privacy, and especially various aspects of personal privacy, have repeatedly been at the center of public discourse. The growing preoccupation with personal privacy stems from the great change [1] Information Communication Technologies (ICT) have brought about in all walks of life in the last two decades. The information revolution hasenabled us totranslate personal privacy into information about personal privacy. Personal privacy can therefore be discussed in terms of personal privacy information. In this article, we will present the fundamental challenges that arise from the fact that personal privacy is information. The challenges can be named: a "physical" challenge that originates from the fact that personal of order, and every order necessarily goes wrong because of the law of naturethat entropy grows in the world. A challenge arising from the essence of information, whatever information that "wants" to disseminate itself in the world. Challenges originating from the structure of the information network and general and psychological factors that accelerate the dispersion of personal information on the network and thus violate personal privacy. And economic reasons that caused personal privacy information to become a commodity.

**Keywords:** Personal Privacy, Deep and General Personal Privacy, personal privacy information dispersible, Personal privacy information as "order", Entropy as the physical basis of the turbulence in personal privacy, network structure on the decrease in order in personal privacy.

### INTRODUCTION

Many attempts have been made to redefine personal privacy, none of them adequate [2,3,4,5,6,7]. In this article, I replace the discussion about personal privacy with discussion of personal privacy information. Based on that, I offer new definitions for deep personal privacy information and general personal privacy information, deep personal privacy is the knowledge one has about oneself minus the knowledge the world (or society) has about one, i.e., the things one knows about oneself - one's body, mind, etc. - that are not known to anybody else. In terms of information, it means information about a person that is possessed by nobody but that person. General personal privacy is the knowledge one and one's confidants have about one, minus the knowledge the world has about one. Confidants have an understandable commitment not to disclose that knowledge publicly (or they would not be confidants), in other words, to keep it in the private sphere. A confidant may be an individual - e.g., a doctor, a psychotherapist, or a family member - or an institution, e.g., an insurance company or a bank. In terms of information, it means information about a person that is possessed by that person and their confidants, but not by anybody else (including other individuals, databases, enterprises, or organizations). In the next section, I'll present the fundamental challenges for the protection of personal privacy, General personal privacy, and deep personal privacy as well, which originate from the fact that personal privacy is information managed by information technologies in the age of ICT (Information Communication Technologies). The challenges can be named: a "physical" challenge that originates from the fact that personal privacy is a kind of order, and every order necessarily goes wrong because of the physical law of entropy growth in the world. A challenge arising from the essence of information, whatever information that "wants" to disseminate itself in the world.

Challenges originating from the structure of the information network and general and psychological factors that accelerate the dispersion of personal information on the network and thus violate personal privacy.

### What makes personal privacy information dispersible [8]

Protecting personal privacy information against public exposure is challenging for two reasons: one, formulated by John Perry Barlow, is that information behaves like a life form [9]; the other, explained by Richard Dawkins, is that information elements are memes, which are similar to genes in that their goal is to replicate [10]. Barlow lists three key characteristics of information that explain why personal privacy information is dispersible by nature [11]:

1. Information is an activity: it is a verb, not a noun; it is experienced rather than possessed; and it has to move (flow). Information that isn't moving ceases to be information or becomes frozen until it can move again. Regarding personal privacy information, information that an individual keeps to themself and that cannot be passed on to other entities, even potentially, becomes irrelevant and meaningless. For example, if you know you are sensitive to a certain smell, but nobody else knows about it and your behavior does not give it away, this information is irrelevant to your interaction with the world; it is meaningless. How information spreads is very different from the distribution of physical goods: it can be transferred without leaving the possession of the original owner. It can replicate itself endlessly and spread without falling apart into little pieces. However, even though the sender of the information does not lose it, they do lose some power (knowledge is power), while the power of the information receiver increases respectively. In the age of ICTs, information in general and personal privacy information in particular is dispersed via physical and virtual platforms (the Internet and social media). Personal

<sup>\*</sup>Corresponding Author: Dr. Yair Oppenheim,

Tel Aviv University, The Lester and Sally Antin Faculty of Humanities, School of Philosophy, Linguistics and Science Studies.

privacy information is being aggregated continuously, with virtually no filtering, and often "sits" until it is needed. Helen Nissenbaum connected information and personal privacy by defining personal privacy as a flow of information [12]. Personal privacy information flows from the sphere of deep personal privacy into the sphere of general personal privacy, and on to the public sphere.

- 2. Information is a life form: This argument is based on meme theory, which was introduced by Dawkins in his book The Selfish Gene [13]. Because information "wants" to flow, as argued by Barlow, every piece of information is also a meme that wants to replicate and spread. This is true of any information, including personal privacy information. For example, when our body "wants" to spread information about itself, it sends out messages that can be perceived by the senses (e.g., sight, smell, touch), or even messages from which our mental state or traits can be inferred<sup>1</sup>. Dissemination of personal privacy information has increased greatly in the age of ICTs. Governments and commercial organizations aggregate pieces of personal privacy information, analyze them, and share them for commercial and other uses. The information is usually replicated many times and stored simultaneously in multiple databases (e.g., every Internet app stores personal information for its own and others' needs), and so the memes replicate and spread, violating both general and deep personal privacy. Other mechanisms, such as entropy and human curiosity, further increase the dispersion of personal privacy information.
- 3. Information is a relationship: Information acquires meaning only when it flows from its source to its recipient. This is the process through which data turns into meaningful information. Further meaning is added by the way the information is stored and presented. For example, a piece of information like your bank account balance has meaning in itself at a given time point, but when presented in a series of your account balances over some time, it can give a much better picture of the state of your financials, whether it has improved or worsened, and where you stand financially compared to other people. Data also acquires meaning through our interactions with ourselves, particularly if we have multiple online and offline identities (whether they exist alongside each other or replace one another). When private personal information flows (or has the potential to flow) from the private sphere to the public sphere, it affects the privacy of the information subject.

As we have seen, personal privacy information is information, and as such, it is a living being and wants to degrade itself to infinity according to meme theory. So, there is a great and growing difficulty in protecting personal privacy.

### Personal privacy information as "order" [14]

In the most general sense, order in any system (whether physical, social, or biological) is when its various parts are arranged according to a particular sequence, pattern, or method with each other – "a law, or a principle, that governs the relations among the parts" [15]. Order can be artificial, i.e., human-made, such as the lexicographical order of books in a

library, or it can be natural–physical, biological, etc., in which case it is referred to as "a law of nature". Either way, order has three main characteristics: complexity, lawfulness, and quantitatively [16].

The term "order" applies to the relationships between the various parts of the system and to the ordering principle that governs them. It can be both internal, defining the arrangement of the parts with each other, and external, defining the relationships between the system parts and entities that are not part of the system. The order may change as parts are added or subtracted, but that does not change the ordering principles (laws) of the system. The degree of order means the degree of a system's conformity to its ordering principles, and so, we can define a system as "more ordered" or "less ordered". Order and disorder are not a dichotomy [17]; most systems are somewhere on the spectrum of conformity between complete order (in physics - zero entropy at absolute zero, in economic and social systems - complete equilibrium) and complete chaos (when the system's ordering principles no longer apply and it bounces from state to state without any ability to reach equilibrium). An information system is in total order (zero entropy) if zero information flows in, out, or through it.

To understand whether personal privacy can be defined as "order", let us examine it through the three characteristics of order: complexity, lawfulness, and quantitatively. There are two aspects of the complexity of personal privacy: one aspect is the relationship between every individual's agency and society, which is comprised of different reference groups and other individuals; the other aspect is the multiple basic components extracted from the various definitions of privacy, which carry information and together make up all our personal (and private personal) information,<sup>2</sup> and the interactions between them. The lawfulness of personal privacy is the system of laws, regulations, and social norms designed to protect personal privacy and personal information, which is an integral part of personal privacy. The personal informationis also measurable and quantifiable under Claude Shannon's information theory [18]. As we can see, personal privacy meets the criteria of order, and therefore, it is possible to discuss the degree of order (or disorder) in personal privacy in the age of ICTs.

The age of ICT has created disorder in major areas of life (politics, economics, society). The shaking of the order can be felt in every aspect of our private lives as well as in the legislation, norms, and ethics regarding personal privacy. The laws of the economy seem to be changing, and it is not yet clear whether the principles and rules of capitalism still stand, or whether we are seeing the rise of a new economic system. The old social order, which guaranteed social welfare and economic growth through a system of balances between the government, the producers, and the workers, is being challenged as well. The result is that in the age of ICTs has personal privacy is in a state of turbulence [19]. The state of disorder of personal privacy in the ICT era can be estimated according to the five parametersthat Ralph Stacey defines for placing a complex system on the spectrum between order and chaos [20]:

<sup>&</sup>lt;sup>1</sup> Some claim, for example, that fear has a smell. The body communicates information using a world 1 indicator (scent).

<sup>&</sup>lt;sup>2</sup> Personal information that isn't private means information about us that is also known to other people, while private personal information is information about us that is possessed or controlled by us.

- The intensity of information flows between the nodes of the system: Tremendous amounts of personal information flow through the Internet every day, which puts the system of personal privacy and personal privacy information high on the spectrum of disorder [21].
- Personal information as the primary resource of the ICT culture is being collected, aggregated, analyzed, and disseminated using a wide range of means, including the IoT, AI systems, smartphones, communication networks, and above all, sophisticated apps they employ all of those. Therefore, for this parameter, the system of personal privacy is also placed high on the spectrum of disorder [22].
- The level of interaction between the nodes of the system, and between the system and the world around it: One of the primary components of the network society is the network human, who is simultaneously a node in the social network and an agent who interacts with the network and affects it. Every individual who is a node in the network extensively interacts with other nodes, exchanging personal and private information. This activity shapes the state of personal privacy. Furthermore, not only are individuals themselves nodes in the network, but their personal information is also contained in multiple devices (such as smartphones, databases, PCs and IoT devices) which are nodes in the network too, and they are all connected through the Internet, constantly interacting, exchanging and updating personal information. Thus, this parameter shows a high degree of disorder, too.
- The system nodes' motivation and involvement level: Because personal information is the primary source of income for large Internet companies, they have very strong motivation to keep using it, and are doing everything they can to remove any legal or normative obstacle that might prevent them from doing so. Governments and other noncommercial organizations also have a motivation to control personal information, as it increases their control and management capabilities. Thus, the fourth parameter also shows a high degree of disorder.
- The system's hierarchical structure: In contrast to the Classical Capitalism era, organizations (whether commercial, political or social) in the network society are typically flat, because the social and technological network allows direct contact between nodes with little need for middlepersons. This leads to the "small world problem" with its maximum of six degrees of separation. This last parameter also puts the system of personal privacy high on the spectrum of disorder.

As we can see, in the age of ICTs, personal privacy as a complex system has a very high degree of disorder. This creates a feeling of chaos, which is intensified by declarations of the death of privacy or of its being unneeded and unjustified, and makes government (and non-government) regulation in this field a matter of urgent priority.

# Entropy as the physical basis of the turbulence in personal privacy

In physics and biology, entropy is defined as the degree of disorder (chaos) in a complex system. American mathematician Norbert Wiener called it "nature's tendency to degrade the organized and destroy the meaningful" [23], with a characteristic tendency to increase. In the specific context of information, he defined the message as "a sequence of events

in time which, though in itself has a certain contingency, strives to hold back nature's tendency toward disorder" [24]. Order in personal privacy information means a clear definition (Paradigm) of the legal regulations and social norms that govern it, and of the entities that should own and control it. These determine the degree of order in personal privacy. An increase in entropy means a decrease in the degree of order. The process of personal information leaking out of the private sphere into the public sphere may be compared to molecules of gas flowing from one container to another until they reach equal pressure, under the second law of thermodynamics. You can imagine the private and public spheres as communicating vessels connected through multiple Internet channels, each containing pieces of information. Due to the properties of information, when it flows from one sphere (vessel) to the other, it replicates itself without leaving the original vessel. As entropy grows, the system will strive toward equilibrium between the vessels and the categories of information each contains.

Since personal privacy can be translated to information, the more information others have about a specific aspect of your privacy, the less uncertainty regarding your personal privacy they have. When personal privacy information leaks out of the private sphere into the public sphere, your level of privacy is decreased. Knowledge about deep personal privacy is always indirect.So, there is always some uncertainty regarding the interpretation and association between the manifestations of personal privacy that are observable in the visible world and personal privacy itself. To measure that uncertainty, the Entropy function is the tool for assessing the actual personal privacy<sup>3</sup>. Here is a numerical example of personal privacy information dispersal:Let us describe the certainty of personal information dispersal as follows: X is a collection of elements of personal information, such as marital status, phone number, age, height, weight, and other elements of information included in the basic components of privacy. p(x) is the probability that information element x resides entirely in the private sphere.

Let us assume that p(x) = 0.67; therefore, 1 - p(x) = 0.33.

This makes the entropy of *x*'s dispersal between the two "vessels" (i.e., the private and public spheres):

 $H(X) = -[0.67\log_2(0.67) + 0.33\log_2(0.33)] = 0.9149$ 

Thus, the certainty I(X) of the dispersal of x in the public sphere is:

$$I(X) = 1 - H(X) = 1 - 0.9149 = 0.0851$$

If ICTs are increasing the probability of x leaking out into the public sphere so that  $p(x) \ge 0.85$ , the entropy will be:

$$H(X) = -[0.85\log_2(0.85) + 0.15\log_2(0.15)] = 0.6098$$

Which means the certainty I(X) of the dispersal of x in the public sphere will be:

$$I(X) = 1 - H(X) = 1 - 0.6098 = 0.3902$$

<sup>&</sup>lt;sup>3</sup>The entropy function:  $H(x) = -\sum p(x) \cdot \log p(x)$ . The entropy function measures the association between the degree of order or disorder in information and its randomness, or uncertainty. It is a major tool used for data mining and for prediction of facts based

There is always uncertainty regarding personal privacy, because it is precisely that gap between what we know about ourselves and what the world knows about us. Formally, the entropy function H(X) is monotonically increasing, which means personal privacy is decreasing. The theoretical lower limit means all the private information is out in the public sphere. This limit is unreachable because, at the very least, deep personal privacy can never disappear. In conclusion, the entropy growth law causes the degree of personal privacy order. On the other hand, the entropy function is a mathematical toolfor measuring personal privacy in each state of affairs.

# The influence of the network structure on the decrease in order in personal privacy

Metcalfe's law states that the financial value of a telecommunications network is proportional to the square of the number of connected users of the system  $(n^2)$ . According to Carl Shapiro and Hal Varian, the value of a network is the number of connections between its nodes [25]; formally: network value  $V = \frac{n \cdot (n-1)}{2}{}^4n$  being the number of nodes. Therefore, if the network value for a single user is \$1, a network of 100 users will have a total value of \$4950.<sup>5</sup> According to the law of large numbers, the network value will eventually asymptotically approach  $n^2$ . The influence of the increase in network value on privacy is that more and more personal information is being dispersed to the other nodes in the network, so that based on Metcalfe's law, the value of privacy can be said to reduce proportionally to  $\frac{1}{n^2}$ . Thus, the value of personal privacy (pp) for all the network users will formally be  $pp = \frac{1}{n \cdot (n-1)}{}^2$ . In a network of 100 users, it amounts to  $\frac{1}{4950} = $0.0002$ .

Stuart Kauffman added to Metcalfe's law the parameters k – the number of connections between the nodes, and p [26]– the rules (norms) of connecting by which each node is guided, and which determine the content that will be exchanged between the nodes.<sup>6</sup>Letus assume that p = 1, i.e., that private personal information is always exchanged; therefore, the number of connections each network user has with other Internet users through ICTs is k < 1.<sup>7</sup> This makes the financial value of the network  $V = k \cdot \left(\frac{n \cdot (n-1)}{2}\right)$ ; respectively,  $pp = \frac{1}{k \cdot \left(\frac{n \cdot (n-1)}{2}\right)}$ .

Thus, the very nature of the network social structure formed in the age of ICTs contributes to the ongoing process of depreciation of personal information. This is in line with the earlier presented conclusion regarding the parameters of order and disorder in personal privacy<sup>8</sup> and with the Internet companies' estimate of the financial value of personal information, manifested in the fact that "users' web browsing history elements are routinely being sold off for less than \$0.0005"[27].

In addition, according to Robert Axelrod, the more two people interact with each other, the greater their mutual trust [28].The same goes for web applications: the more we use an application, the more we trust it. This explains the indifference with which people provide elements of their personal information to web apps: they believe, based on cumulative personal experience, that the apps are trustworthy and are using the personal information fairly to optimize their services, without really violating users' privacy. However, this is usually an illusion, as explained in the section about the network market, which exploits our personal information for profit with little or no consideration for our privacy [29]. The conclusion that follows is that the psychology of people's online behavior is another factor that contributes to increasing violations of and disorder in personal privacy.

The conclusions are: The structure of the network and the strength of the connections between the network nodes is that the network is growing (i.e. it has more nodes and there are more connections between the network nodes). Because the economic value of the network is increasing for the big Internet companies (Facebook, Google, Amazon.) On the other hand, the economic value of a piece of information for the end users (network customers) is decreasing. So the interests of the network companies in collecting and processing, and disseminating personal informationare growing. On the other hand, for the individual, the value of his personal information is very small until he is ready to give it away for free. And so the Internet network structure and the economic interests of the big Internet companies contribute to the difficulties of protecting personal privacy.

#### The network economy violates personal privacy

Network production, network work, and the network market create a new kind of economy - the informational economy [30]. According to Roland Kley, the new economy is essentially communication-based, the Internet being its dominant technology, which allows every individual to become a node in the economic network and to communicate with other nodes in order to perform their financial operations [31]. The new economy uses network technology to remove the obstacles (norms and regulations) between the individual and the market. Our personal information has become the essential fuel that powers the network economy. The process of using personal information to fuel the network market has two stages, between which there is continuous feedback: the first stage is obtaining personal information, and the second stage is using it to power the industry. Shoshana Zuboff explains that the initial purpose of collecting personal information was to improve the quality of services [32], but with time, Internet companies - first Google, then others such as Facebook and Netflix - began to realize that the "behavioral surplus" was an essential economic resource for them, because the aggregation and analysis of user information helped them accurately predict consumer wishes and preferences, allowing targeted advertising, and eventually also niche production and niche marketing. That was the very resource that helped Internet companies thrive and survive the dot-com crash of the early 2000s. This, according to Zuboff, was the beginning of surveillance capitalism: "Google discovered that we are less

<sup>&</sup>lt;sup>4</sup> Based on the combinatoric calculation that if a network has *n* nodes, they are theoretically connected by  $\frac{n \cdot (n-1)}{2}$  edges.

<sup>&</sup>lt;sup>5</sup> Facebook allows each user a maximum of 5000 friends – a limitation one can bypass by using multiple online identities.

<sup>&</sup>lt;sup>6</sup> For example, the criteria you use to decide whether to accept or ignore a Facebook friend request, or whether to allow an app to use your location data.

<sup>&</sup>lt;sup>7</sup> E.g., the number of web applications – such as Instagram, Twitter, Facebook, Google Search, etc. – one is using.

<sup>&</sup>lt;sup>8</sup>The intensity of information flow between the nodes, the variation in operation modes, the level of interaction between the nodes, the nodes' motivation and involvement level, and the system's hierarchical structure (the Internet network supports a flat organizational structure).

valuable than others' bets on our future behavior." [33]. This discovery has transformed the network market and network economy. Consumers are profiled using an arsenal of surveillance and monitoring tools that monitor them continuously, both in the physical and virtual spheres. Individuals are usually unaware that they are being monitored, and even if they are aware of it, they cannot avoid it [34]. One example of a service that collects personal information with nothing the consumer can do to prevent it is mobile payment systems and shopping apps. However, consumers tend to prefer unobtrusive targeted ads to obtrusive ones, regardless of the actual extent of personal privacy violation.

The advent of ICTs gave rise to big data pools, which have become a separate ecosystem that allows storage, fusion, analysis and dissemination of personal information as part of economic models that treat it as a commodity. The market of personal information is controlled by a handful of Internet corporations such as Facebook, Google, Amazon and a few more. The consumers are provided with free products and services, and in return, their personal information is made into a commodity traded on the network market. The Internet companies justify it by claiming they are serving the common good and contributing to an open society in which both consumers and merchants have access to the right selection of options so that each can make the best decisions for themselves [35]. This argument is used to justify targeted advertising, which supposedly bridges between a consumer's preferences and the produced supply.

The conclusions are: The network market and of surveillance capitalism use personal information (including private personal information) as the raw material of the network market economy andare being used by the players in this market for profit or to achieve social and political goals. The use and commodification of our personal information take it out of our control and puts it under the control of the players in the network market. By definition, network market resides in the public sphere, which, driven by the market's economic and political interests, penetrates the private sphere until the distinction between the two is blurred. As a result, increasing amounts of personal privacy information and deep personal privacy information become exposed to the public.As we saw in a previous section, as the individual's participation in the network economy increases, so does his trust that this economy serves his economic good, that giving up his personal privacy to an increasing extent is a worthwhile price.

### Conclusion

When personal privacy is translated into information about personal privacy, as is happening in time in the age of ICT. The ability to protect personal privacy is severely challenged by the characteristics of the ICT age. The challenging characteristics for personal privacy are:

- The information itself has the characteristics of a living entity that wants to reproduce endlessly
- The personal privacy paradigm is a type of order that, like any order in the world, is being undermined by the law of entropy growth.
- The network structure in which the human individual operates in the Internet.Supports and rewards the creation of connections and transfer of information between the network nodes. The larger and more complicated the

network, increases the social and economic value of the network itself, and at the same time, the decreasesthe social and economic value of the single piece of information.

- Theinformation in general is the economicfuel of the ICT. In particular the personal privacy is a resource that is used to increase the profit of the large network companies. Therefore, personal privacy has become a commodity that changes hands in the market of goods that is conducted in the public sphere.
- Psychologically, as the individual intensifies the use of the Internet, his trust in the Internet increases, and the sense of danger in revealing his personal privacy decreases. Therefore, he is ready to give up personal privacy, if in return he receives the application services of the network companies.

Each of these challenges is enough to severely disrupt personal privacy. All the challenges together cause the justified feeling that in the age of ICT it is no longer possible to protect personal privacy. To deal with the great challenges to personal privacy that the characteristics of the ICT age pose, a new personal privacy paradigm must be designed that re-examines the possible answers to these challenges. I think we should concentrate on protecting deep personal privacy.

### REFERENCES

- 1. Alvin Toffler, *The Third Wave* (New York: Morrow, 1980), 17.
- Ferdinand D. Schoeman, "Privacy: philosophical dimensions", in: *Philosophical Dimensions of Privacy: An Anthology*, ed. Ferdinand D. Schoeman (Cambridge: Cambridge University Press, 1984), 3.
- 3. Graeme Laurie, *Genetic Privacy: A Challenge to Medico-Legal Norm* (Cambridge: Cambridge University Press, 2002), 6.
- 4. Soraj Hongladarom, *A Buddhist Theory of Privacy* (Singapore: Springer Singapore, 2016), 16.
- 5. Ruth Gavison, "Privacy and the Limits of Law", *The Yale Law Journal*, Vol. 89, No. 3 (January 1980), 421.
- 6. Daniel J. Solove, *Understanding Privacy* (London: Harvard University press, 2009), 1-2.
- 7. Helen Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life (Stanford, Calif.: Stanford Law Books, 2010), 16.
- 8. Oppenheim Yair, Personal Privacy in the Age of the Internet, Spines, 2024), 236-239
- John Perry Barlow, "The Economy of Ideas", Wired Digital, Inc., 01/1994, 1-15. https://www.wired.com/1994/ 03/economy-ideas/ (Accessed 22/8/2020)
- 10. Richard Dawkins, *The Selfish Gene* (Oxford: Oxford University Press, 1976).
- 11. Barlow, "The Economy of Ideas".
- 12. Nissenbaum Helen, Privacy in Context: Technology, Policy, and the Integrity of Social Life (Stanford, Calif.: Stanford Law Books, 2010), 127
- 13. Dawkins, The Selfish Gene, 245-260.
- 14. Oppenheim Yair, Personal Privacy in the Age of the Internet, Spines, 2024), 339 246
- Ruth Lorand, Aesthetic Order: A Philosophy of Order, Beauty and Art (London and New York: Routledge, 2000), 9.
- 16. Ibid., 9-19.
- 17. Efron Razi and Pinhas Yehezkeally, *Ha-olam eino liniari:* Torat ha-maarakhot ha-merukavot – gorem khadash be-

*nihul* [Real Life Is Not Linear: Introduction to Complex System Theory] (in Hebrew) (Tel Aviv: Ministry of Defense Publications, 2007), 68-71.

- Claude E.Shannon, "A Mathematical Theory of Communication", reprinted with corrections from *The Bell System Technical Journal* Vol. 27 (October 1948), 12.
- 19. Razi and Yehezkeally, *Ha-olam eino liniari...*, 71-72. A physical state in which a system's behavior is unpredictable even though all its ordering principles are known.
- 20. Razi and Yehezkeally, Ha-olam eino liniari..., 174.
- 21. From the 2017 Database Registrar Report by then Commissioner of the Privacy Protection Authority Adv. Alon Bachar, November 2018, Ministry of Justice – Privacy Protection Authority, pp. 5-6: "The extensive amount of personal information that is being collected includes our interests, daily activities, desires, ambitions, preferences, dreams, and the people we are in contact with. All this information is being systematically and efficiently processed and aggregated to create detailed, segmented personalized profiles".
- 22. Ibid.: "Every area of our daily life is associated with sophisticated technologies and increased exposure of our information online. Living in the digital age means our every action, or inaction, leaves a unique digital footprint which includes information about every place private or public we have visited, and every website or app we have used at home, at work, on the street, from our mobile phone, smart watch, TV set, car, smart toy, etc. [...] All this information is being systematically and efficiently processed and aggregated to create detailed, segmented personalized profiles which are used, and even sold to third parties, for a variety of commercial, political and other purposes. The information is often collected without our full knowledge and without our free consent."
- 23. Norbert Wiener, *The Human Use of Human Beings: Cybernetics and Society*(New York: Da Capo Press, 1954), 158.

24. Ibid., 27

- 25. Carl Shapiro and Hal R. Varian, *Information Rules: A Strategic Guide to the Network Economy* (Boston: Harvard Business schoolpress, 1999), 184.
- 26. Razi and Yehezkeally, Ha-olam eino liniari..., 123.
- 27. Lukasz Olejnik, Tran Minh-Dung and Claude Castelluccia, "SellingOff Privacy at Auction", 23-26.
- Robert Axelrod, The Evolution of Cooperation (New York: Basic Books, 1984), 174-175.
- 29. Shoshana Zuboff, *The Age of Surveillance Capitalism* (London:Profile Books, 2019), 178.
- 30. Manuel Castells, *The Rise of the Network Society*, Preface to the 2010 edition, xvii. 163
- 31. Roland Kley, *Hayek's Social and Political Thought*(New York:Oxford University Press, 1994), 256-259, 262-263.
- 32. Zuboff, The Age of Surveillance Capitalism, 70.
- 33. Ibid., 93.
- 34. Chris Jay Hoofnagle, Jennifer M. Urban and Su Li, "Mobile Payments: Consumer Benefit & New Privacy Concerns", SSRN Electronic Journal, April 24, 2012. https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=20455 80 (Accessed 4/5/2021)
- 35. From Mark Zuckerberg's speech at Georgetown University: "I remember feeling that if more people had a voice to share theirexperiences, maybe things would have gone differently. Those earlyyears shaped my belief that giving everyone a voice empowers thepowerless and pushes society to be better over time". Appeared in: Tony Romm, "Zuckerberg: Standing for Voice and Free Expression", *The Washington Post*, 17 October, 2019 https://www.washingtonpost.com/technology/2019/10/17/z uckerberg-standing-voice-free-expression/ (Accessed 4/5/2021)

\*\*\*\*\*