International Journal of Science Academic Research
Vol. 06, Issue 06, pp.10163-10170, June, 2025
Available online at http://www.scienceijsar.com

ISSN: 2582-6425

Research Article

PERSONAL PRIVACY INFORMATION

***Dr. Yair Oppenheim**

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

Received 15th April 2025; **Accepted** 20th May 2025; **Published online** 20th June 2025

Abstract

This paper examines personal privacy in the era of Information and Communication Technologies (ICTs). It identifies the basic components of privacy [1], such as Body, Mind, Actions, Property, Relationships with external entities, Identity, and Anonymity. The sources highlight how ICTs have profoundly increased the collection and aggregation of information connected to these fundamental components. It is posited that personal information is not a separate component but comprises the informational elements within each basic privacy component. The text proposes redefining the private sphere using information and knowledge, distinguishing between deep and general personal privacy. The central argument is that replacing the discourse on personal privacy with one on personal privacy information is justifiable, supported by several points: personal privacy information can be digitized and detached [21] from the individual; personal privacy is fundamentally viewed as personal privacy information; and any discussion about personal privacy is, in essence, a discussion about this information. Furthermore, individual personal privacy is differentiated by respective personal privacy information. The paper also establishes that personal privacy information meets the criteria for being information according to Floridi's definition and is a well-defined concept [17], aligning with established data categories. Therefore, the sources conclude there is no logical obstacle to this conceptual replacement, asserting that personal privacy information is measurable and quantifiable [1], with ICTs facilitating its storage, processing, analysis, and dissemination.

Keywords: Personal Privacy, Deep and General Personal Privacy, basic privacy components, private sphere, public sphereEntropy as the physical basis of the turbulence in personal privacy, network structure on the decrease in order in personal privacy.

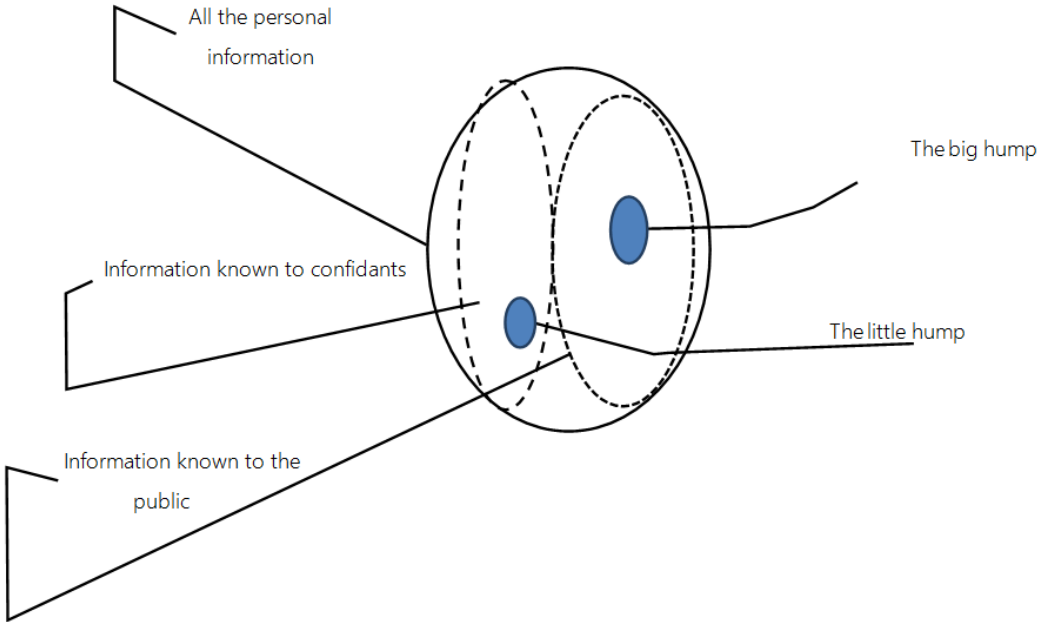
INTRODUCTION

The basic privacy components are: Body (including genetic data), Mind (thoughts, emotions, preferences inferred from behavior), Actions. Property information, Relationships with external entities. Identity (Our identity is the product of our unique individuality) and Anonymity, Different types of anonymity are discussed (e.g., donation, medical, communication, commercial, and expression) ICTs have substantially increased the collection and aggregation of information related to the basic privacy components. Personal information is not a distinct component of privacy; rather, each of the basic components of privacy carries elements of information. All the components of personal information combined make up all of one's personal information. Before the age of ICTs, information was stored in analog formats written (whether handwritten or typewritten), photographic, or recorded and could be perceived and understood by direct use of our senses, mainly sight and hearing. There was no shared platform, making it difficult to connect different pieces of information. In the age of ICTs, analog storage was replaced by digital storage. The digitization of information and its storage in large data pools connected through a shared platform – the Internet – allowed for making connections between different pieces and categories of information without dependence on their physical location, and often without dependence on time. This change had an enormous impact on the distribution of information in general, and the distribution of personal information in particular. Nowadays, personal information about every human being worldwide is being stored and aggregated.

Corresponding Author:** ***Dr. Yair Oppenheim,
Linguistics and Science Studies, School of Philosophy, The Lester and Sally Antin Faculty of Humanities, Tel Aviv University, Israel.

Information can be viewed in its digital form and analyzed by machines without any need for human senses. It is distributed in multiple copies and can be analyzed and understood without any help from human eyes or ears[1]. Moreover, upuntil recently, most personal information had a limited "life span" that roughly corresponded with the lifetime of the data subject, but now, information can survive much longer than the individual it refers to. Let us redefine the private sphere in terms of information and knowledge and define deep personal privacy as the information about one's body, mind, etc. that nobody except oneself knows, i.e., the knowledge one has about oneself minus the knowledge the world (or society) has about one. General personal privacy is the information about one that is shared by one and one's confidants, but not by the world in general (other individuals, databases, enterprises, or organizations) – in other words, 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 this knowledge publicly and to keep it in the private sphere – or they would not be confidants. 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. Those are the formal definitions of the private sphere in terms of information and knowledge, or what Westin calls "social distance". Deep personal privacy is not available by direct observation of that world, but is inferred based on information from conscious reports using speech, writing or art (drawings, music, dance); unconscious reports such as physical symptoms (odor, sweating, movements or body temperature); or indirect reports (e.g., family pictures which inadvertently reveal information about the relationships in one's family).

[1] The transition from information collection by people (human net) to information collection by machines in government and military organizations is a proof of that.



That information is analyzed based on science and knowledge. No information element can be placed exclusively in the sphere of deep personal privacy, general personal privacy or the public sphere. The relationship between deep privacy, general privacy, and personal information in general in the age of ICTs can be represented by the following graph. The outermost oval represents all the personal information about an individual, the dashed oval represents the personal information known to confidants, and the dotted oval represents the personal information that is known to the public. The relationship between the various types of personal information is changing due to the ICTs' increasing ability to expose personal information that was previously considered private. The exposure of personal privacy information creates the "humps" – information about the individual that is known to others (one or more confidants, or the general public), but not known to, possessed by or controlled by the individual who is the information subject.

Personal privacy information carried by each of the basic components of personal privacy

Body: The body component includes physical characteristics such as appearance, height, weight, strength, health, senses, etc. Every one of those can be translated into information. Some physical information related to our body is stored in medical databases in the form of photographs or measurable values. Other elements of body-related information, such as appearance, age, and gender, are stored in photographs or government databases such as population registers.[2]Somebody-related information can only be stored and aggregated thanks to ICTs, like results of personalized genetic testing, which has become possible after the completion of the Human Genome Project. The documented genetic data of millions of people is used for a variety of purposes, including the discovery of genetic variations that may cause diseases, the identification of criminals, and the testing of potential partners. Today, all the information related to our body and its properties is digitally recorded and aggregated.

Whereas before the age of ICTs most of that information would expire with the person, nowadays it can survive long after the person's death and decay of the body.[3] Some elements of body-related information reside in the sphere of general personal privacy and are only shared with chosen confidants – e.g., our private parts, genetic information, and other health information. Body-related information not known to anybody but ourselves resides in the sphere of deep personal privacy.

Mind: The abstract, virtual part of a human being which contains our thoughts, emotions, pains, desires, sense of self, memories, and other mental elements such as inhibitions, fears, weaknesses, and mental health conditions. All these elements turn to information when expressed through speech, writing, art (drawings, music, songs, or dance), body movements, or the positioning of the body. Until the age of ICTs, most of that information was short-lasting, with a little of it retained in analog formats such as writings, voice recordings, or works of art. However, these days, vast amounts of mind-related information are being aggregated in digital databases. Mental elements which had never been recorded until the age of ICTs include our culinary preferences, which are recorded in the databases of food retailers, and our hobbies and interests, inferred based on our shopping habits [2]. Human behavior is being recorded and turned into digitally stored and aggregated information [3]. A large portion of mind-related information is obtained from indirect sources. The ICTs combined with databases) can together uncover people's inner world, defined as deep privacy. The majority of mind-related information resides in the sphere of deep personal privacy; the parts we choose to share with confidants reside in the sphere of general personal privacy. The ICTs transfer mind-related information from the private sphere to the public sphere.

Actions: ICTs allow for constant monitoring of everything people do, both in the physical and virtual space. Most of our actions leave footprints in the physical space, which are collected and stored in large, interconnected databases. Vast

[2] A person's health can be translated into various measurable factors such as blood pressure, heart rate and blood sugar.

[3] Digital systems forget nothing, and that raises questions regarding posthumous privacy – questions which had seemed irrelevant before the digital age.

amounts of information are collected through our smartphone – when we are active (using apps), but also when we are not actively using it – and through a wide range of devices and sensors such as CCTV cameras (commonly used in "smart cities" [4]), private web cameras, geolocation satellites that can locate a particular person in the physical space at any given moment, and "cookies"[5] planted in our PCs and smartphones to monitor our behavior in the virtual space. Until the age of ICTs, people's actions were hardly documented at all, but today, our movements in the physical space are recorded by apps like Waze and various proximity tracing app.[4], our shopping habits are traced based on our credit card activity [6], our interests can be found out based on what we order online and our surfing patterns (the websites we visit, the amount of time we spend on them, and our emotional responses to the content we see) [7], there are records of our typing behavior, phone and Internet communications,[5] eating habits,[6] movie preferences, participation in social events such as weddings or rallies, and many more. As we will see, most of those records are indirect information that is being used by government and political organizations (such as intelligence and security agencies) as an aid for making political decisions, or by commercial organizations as an aid for making commercial decisions. Most of the things people do as agents who interact with the physical world are visible and observable in the public sphere; some things are shared exclusively with confidants, and thus belong in the sphere of general personal privacy; while things only the person in question knows they did reside in the sphere of deep personal privacy, and as far as everybody else is concerned – might not have been done at all, or at least not by that person.[7] However, this changes when information about actions intended to be kept in deep personal privacy becomes known to others.

Property: The concept of property includes one's body and mind, of which one is the sole owner; the physical space in which one can do whatever one likes; and the products of one's mind, including abstract ones such as thoughts and memories. Property-related information has been recorded and stored since the dawn of civilization, especially since the invention of writing, but most of it would expire with the owner – i.e., most property-related information was inseparable from its container. Information related to intellectual property focused until the age of ICTs on copyrights and patent rights – products of world 2 manifested mainly in world 3. Privacy information such as feelings, intimate relationships and body-related information has been recognized as property long before the age of ICTs. This kind of property-related information belongs in the sphere of deep personal privacy, and until the age of ICTs, its recording had been minimal and limited to confidants. ICTs allow such information to be recorded and digitally stored in interconnected online big data pools. For the first time in history, property-related information can be separated from its owner and get a life of its own.

External entities: Other players in the system of balances between the protection and violation of one's privacy. External entities include one's confidants, and may be individuals or organizations (e.g., commercial companies, governments, or social networks such as Facebook and Google). External entities possess private personal information about one, including intimate information, information deemed confidential by social norms, and information whose confidentiality is protected by law, like doctor-patient confidentiality or attorney-client privilege. The massive sharing of privacy information on social media in the age of ICTs has greatly increased both the number of online entities who possess our private personal information, and the amount of private information possessed by external entities,[8] in a way that is unprecedented in its scope and in its impact on personal privacy and our ability to protect it.

Relationships with external entities: The nature of the relationships between an individual and other entities. Personal privacy information about personal relationships includes the intensity of the each relationship (usually measured by the amount of time invested in the relationship, its emotional strength, level of intimacy and extent of mutuality[9]), the number of entities with which one communicates directly or indirectly, the methods of communication (e.g., email, phone or WhatsApp), the power relations between the parties, and the kind of privacy information communicated by one of both parties to the relationship. While before the age of ICTs information about relationships with other entities – e.g., meetings with confidants – was usually documented only partly and in analog formats, with social and intimate relationships mostly not documented at all, nowadays most of that information is recorded and stored in big data pools using the means we have already discussed. The information can be direct – e.g., images obtained from security cameras, "bugged" phone calls or intercepted emails, or indirect – such as the number of relationships, the type of information exchanged, and its flow direction. Information about relationships with external entities belongs in the sphere of general personal privacy because it is also known to the other party (or parties) to the relationship. External entities and one's relationships with them make up one's social network of privacy.

Autonomy: The ability to control and make independent decisions concerning one's own body and mind without any external intervention. All three aspects of autonomy – personal, moral and political – are part of world 2, and therefore, any information regarding a person's autonomy can only be obtained indirectly: inferred based on that person's actions and overall behavior, on the behavior of external entities – which obviously affects the autonomy of the person in question, and on other indirect information collected about that person. Autonomy is undoubtedly an essential component of privacy, but despite that, most of the information related to it is out in the public sphere, with only some part of it residing in the sphere of general personal privacy.

Identity: Our identity is the product of our unique individuality, and we have the right to express it and live it out [8], for even though every individual is made up of the same universal building blocks (such as common human physiology,

[4] Digital proximity tracing and contact tracing apps came into public awareness during the COVID-19 pandemic as tools used by governments to prevent spread of the disease.

[5] Which can give a picture of our social contacts.

[6] By means of apps like DayTwo – a personalized nutrition app for people with type II diabetes developed by the Weizmann Institute of Science.

[7] E.g., if it is known that a theft has been committed, but the identity of the thief is unknown.

[8] Nearly every smartphone app records the physical location of the phone user, and I have already mentioned the constant and unstopping recording of our activities by IoT devices and social networks.

[9] E.g., knowing whether the other knows something about us.

genetics and cognitive abilities), the particular combination of those, together with every person's unique history, is what creates each individual's unique selfhood [9]. According to the liberal democratic approach, this special right must be protected. I will use Raffaele Rodogno's definitions of the various "identity questions" to define which information is carried by the identity component of privacy [10].

1. Passport identity: Carries basic bureaucratic information such as identification number, passport number, and/or social security number. Until the age of ICTs, this information had been stored in analog format or designated digital databases such as population registers and tax authority registers; today, it is replicated and disseminated among multiple interconnected databases. One can use passport identity information as a unique identification key to connect different databases. We also have new biometric means of unique identification, such as face recognition, DNA, and identification by IP (Internet protocol) address of a computer or mobile phone.
2. Numerical identity: Identity based on one's cognitive abilities. Information about our cognitive abilities is recorded and stored in IQ tests and report cards from preschool to university. Before the age of ICTs, it was stored in analog formats or in designated digital databases of schools and military systems; nowadays, it can be accessed in all those databases using passport identity information.
3. Attribution identity: Before the age of ICTs, information related to attribution identity was mostly stored in databases controlled by official entities, such as population registers, tax authority registers, banks, and social welfare institutions. Those databases were isolated and mostly static islands of information updated only in case of major life events like marriage, divorce, childbirth, and death. In the age of ICTs, the monitoring of our actions, location, shopping habits, and other patterns of behavior allows for aggregation of all these data as information in interconnected big data pools.
4. Social function identity: Until the age of ICTs, information about this type of identity had hardly been stored or aggregated. Small parts of it were stored in population registers or appeared in passport identity information (e.g., gender and ethnicity). Today, ICTs allow people to assume different identities in different applications, and sometimes more than one identity in the same application, and to present different faces depending on the place, time and other circumstances. On the other hand, the constant monitoring of people's activities by means of ICTs allow for aggregation of data in interconnected big data pools, and AI technologies are used to build profiles based on that data in many Internet-based applications. The advanced AI technologies combine the different profiles into a single nearly complete identity which can be associated with a specific individual, violating their personal privacy. There is an "arms race" of sorts between individuals' ability to assume multiple distinct identities, and the technological capability to unify them, voiding the individual's efforts. Currently, the technological capability to make a link between the same person's different identities seems to prevail over the human attempt to maintain multiple identities [11].
5. Attachment identity: This type of identity resides almost entirely in the sphere of deep personal privacy; any information about it can exist outside our body and mind only if we choose to share it, usually only with confidants. Later, I will show how ICTs can help expose parts of this information, violating people's personal privacy.

Anonymity: According to Pfitzmann and Hansen, anonymity of a subject means that the subject is not identifiable within a set of subjects (the anonymity set) [12]. As I have already mentioned, anonymity violation capabilities have greatly increased in our time due to ICTs' ability to store, distribute, and connect pieces of indirect information about people, eventually allowing their identification. Anonymity violation has two stages: at the first stage, a person's identity is revealed; at the second stage, that identity is associated with a specific individual to physically get to them. I will use Michael Birnhack's definitions of different types of anonymity to describe the information carried by each type and the players engaged in it [13. One thing that is common to all the types of anonymity is the sense of anonymity as anonymity of information. Birnhack lists several categories of social anonymity:

Anonymity of donation: In charity donations, the donor, the recipient, and sometimes both may remain anonymous. Sometimes donations are mediated by charity organizations, usually as a way to increase anonymity. The same type of anonymity applies to welfare payments, in which the mediator is the government, the "donor" is society as a whole – which remains anonymous because no specific welfare payment can be associated with any specific taxpayer, and the recipient is anonymous because social norms dictate that welfare payments should be confidential.

Anonymity of bodily donations: Including gamete, organ, bone marrow and blood donations. The donor usually remains anonymous, and sometimes the recipient does as well. The donation is almost always mediated by a medical institution to ensure physical compatibility. The same institution usually also performs the medical procedures required for the donation.

Anonymity of exams in academic institutions: According to the academic norm of anonymous exams, student exams are checked and graded without knowledge of the student's identity. The anonymity is one-sided, as the professors who grade the exams are not anonymous. The institution's office is a confidant that knows both parties.

Anonymity of peer review: Applied in academic publications and scientific journals. The anonymity is mutual: the authors and the reviewers are anonymous to each other. The process is always mediated by a bureaucratic entity that knows the identities of both parties.

Anonymity of tenders: Bids are submitted anonymously to ensure the entire decision-making process is free from bias, conflicts of interest, and other irrelevant deliberations. The process and the identities of the tender committee are not anonymous.

Anonymity of medical tests: The anonymity of the patient is maintained in medical tests, especially tests for diseases for which one may be subject to discrimination (e.g., at work), shaming, or social stigma. The anonymity applies both to the fact of the test performance and to the identity of the patient. In the age of ICTs, this type of anonymity is at great risk because

medical data is aggregated and stored in interconnected databases, which makes it very easy to associate a test with a specific patient.

Anonymity in therapy groups: Therapy groups, such as Alcoholics Anonymous, maintain the anonymity of their members from anybody who is not a member of the group. The support group becomes a confidant in this case.

Commercial and consumer anonymity achieved by using cash: The majority of commercial transactions that involve the exchange of money or goods are documented. Documentation of trade relations began during the Industrial Revolution and the rise of nation-states. According to Frank Webster and Kevin Robins, scientific management of industrial, commercial, and economic systems (Taylorism) is impossible without an information system such as double-entry bookkeeping. However, this compromises consumer anonymity by extending the circle of confidants to include banks, tax authorities, and other regulatory agencies, who document and store each party's passport identity at the very least [14]. Before the age of ICTs, people would pay in cash to maintain their consumer anonymity, and could thus avoid identification; however, nowadays, commercial and consumer anonymity is increasingly violated, and Internet companies and social media exploit it to maximize their profits. Recent government regulations aimed at battling tax evasions from black market deals greatly limit the use of cash. On the other hand, the advent of virtual currencies allows for anonymous transactions.

Anonymity of communication: ICTs have had a major impact on our ability to communicate anonymously. The ICT properties make anonymous communication virtually impossible. Birnhack focuses on the anonymity of personal communications, applied both to the fact of communication and its content. In this kind of communication, the parties are each other's confidants [15]. Until the age of ICTs, anonymous communication could be face-to-face, by phone (free from third-party listeners), or by post, where the anonymity of the content was protected by a sealed envelope. As already mentioned, this has completely changed in the age of ICTs. Anonymity of customer-vendor communications has also become impossible to maintain, because most of it is being mutually recorded. Above all, the characteristics of our communications cross-referenced with metadata such as our web surfing patterns, consumption habits, and geographical location can be used to create individual users' profiles with the aid of AI tools, leading to a violation of all the various types of anonymity.

Contextual Integrity [16]. It is out of this manuscript.

Anonymity in legal procedures: Publication of suspect names and the very fact of a legal proceeding can be prohibited. A trial may be conducted behind closed doors, without any public disclosure of the details of the case and the legal process. The parties involved, their attorneys, the courts, and law enforcement agencies serve as confidants. Anonymity may be applied to the suspect's or defendant's identity and/or to the details of the offence.

Civic/political anonymity: The right to confidentiality of political opinion and to secret elections. In the age of ICTs, this type of anonymity is being challenged by the use of AI technologies on cross-referenced data from big data pools.

Civil anonymity: The right and ability to make an anonymous report to law enforcement agencies, anonymous whistle blowing, and reporter source confidentiality. The whistleblower or source remains anonymous to those they are reporting against and has confidants. The reported act and the people who supposedly committed it are not anonymous.

Anonymity of expression: Applicable mainly to web and social media activity, including "active" activities such as blogging, posting, and responding to other people's posts, as well as "passive" activities such as web surfing. It is clear why people may want to remain anonymous when using "delicate" web services such as dating and pornographic sites, but some also choose to do their online shopping anonymously so as not to reveal their consumption preferences. Using a pseudonym online allows people to express themselves freely and say whatever they think without filters (whether this is necessarily a good thing is a different question) and with minimal social and other risks. In their strife for online anonymity, people create online identities that seem to have a life of their own. Thus, on the one hand, the age of ICTs has opened up new opportunities for anonymity, but on the other hand, the same ICTs constantly violate that anonymity. There is an "arms race" of sorts between individuals' desire to maintain and protect their anonymity, and others' desire to violate it, and right now, anonymity seems to be losing. Anonymity in its broadest sense includes not only one's identity, but also one's social connections, activities, etc. All the basic components of personal privacy – and accordingly, the information they carry – deserve the amount of anonymity that is accepted in the culture in question.

Personal Privacy Information Qualifies as "Information"

Does privacy information meet the criteria that define an entity as information? Because the word "information" has many different meanings and definitions, I will here use Luciano Floridi's general definition of information (GDI) [17]. According to Floridi, entity α is an instance of information if and only if:[10]

1. It contains N data ($N \geq 1$);
2. The data are well-formed;
3. The data are meaningful.

The first criterion is that information should be made up of data, i.e., it cannot be dateless. The absence of a particular datum does not cancel existing data, but rather provides additional information.[11] Anonymity, for example, is the absence of data. In the previous sections, I described the association between the basic components of privacy and privacy information, the categories of personal privacy data, and the way ICTs collect and store that data in big data pools. Thus, personal privacy information meets the first criterion. The second criterion requires that the data be well-formed, i.e., organized according to the rules (syntax) that govern the chosen system. Syntax here must be understood in its broadest sense as what determines the form, construction, composition, or structuring of something, and may mean code, musical

[10] We will see how all privacy information meets these criteria.

[11] For example, if I do not know the cause of a person's death, it does not cancel my knowledge of the fact they died, or the existence of a cause of death in general. Rather, it means a cause of death exists, but is currently unknown.

notes, or signs on a mechanical drawing, and not necessarily the syntax of a language. The paradigm [18] of personal privacy, which frames all the main conceptions of personal privacy, includes symbolic generalizations, which are the syntax according to which privacy information is organized. Thus, personal privacy information also meets the second criterion. The third criterion is that the data should be meaningful, i.e., comply with the semantics of the chosen system. Floridi makes a distinction between the information's meaningfulness and our ability to understand its meaning [19]. The values and metaphysical parts of the paradigm of personal privacy give privacy information meaning in terms of protection and violation of personal privacy; we can see how the six conceptions of personal privacy, on the one hand, include the various categories of personal privacy information, and on the other hand, represent the metaphysical parts of the paradigm of personal privacy. Thus, personal privacy information also meets the third criterion of the GDI.

Privacy information is a well-defined, objectively valid concept

Due to a lack of a clear and extensive definition thereof. To overcome this difficulty, I am proposing to replace the discussion of the influence of ICTs on personal privacy with a discussion of the influence of ICTs on personal privacy information, a concept that is much clearer and measurable. Let us now see how each category of personal privacy information can be associated with one or more of the five categories of data defined by The Stanford Encyclopedia of Philosophy [20].

1. Primary data: Usually obtained through indicators, e.g., high temperature is an indicator of illness. The categories of personal privacy information that contain primary data are body-related information, information about actions, information about mental and psychological factors, and identity-related information.

2. Secondary data: Data whose absence is what provides information and meaning. Anonymity information is the category that contains most secondary data, as its very nature is an absence of identifying information. Absence of data can also provide information about relationships with external entities, actions (in particular – inaction), decisions and values.

3. Metadata (data about data): In the context of personal privacy information, metadata includes information that defines one's identity, for example, information about interactions with other people that defines one as selfish, or one's actions and decisions that define one as a criminal. Because metadata is a subtype of personal privacy information, and does not belong in any specific information category, they are not included in the summary table below, but it do qualify as personal privacy information.
4. Operational data: Data that has operational use. Include private space information, passport identity information, and information about the values that guide one's decisions and actions (autonomy information).
5. Derivative data: Data that is derived and can be logically inferred from other data. This includes indirectly obtained mind-related information, body-related information inferred from physical indicators (e.g., presence of illness inferred from high temperature), information about actions or decisions inferred based on their observable consequences, indirect information about relationships with external entities, and identity-related information revealed based on other data.

The following table summarizes the classification of the categories of personal privacy information by category of data as defined by The Stanford Encyclopedia of Philosophy. A "V" in a cell means that the information category in the corresponding row includes the data category in the corresponding column. As you can see, personal privacy information categories can be aligned with the Stanford Encyclopedia of Philosophy definition of data categories. This means personal privacy information is a well-defined concept.

The ontological questions regarding the privacy information

Can personal privacy information be detached from its physical vessel, i.e., the individual?

Until the age of ICTs, personal privacy information had normally been attached to and inseparable from the individual,[12] and expired with them (unless the individual was a public figure, in which case parts of their personal privacy information were preserved in history books).

		Category of data			
		Primary data	Secondary data	Operational data	Derivative data
Category of personal privacy information	Private space information			V	
	Body-related information	V			V
	Mind-related information	V			V
	Information about actions	V	V		V
	Property information	V		V	
	Information about external entities			V	
	Information about relationships with external entities		V		V
	Information aboutthe valuesthat guide decisions and actions (autonomy information)		V	V	V
	Anonymity information		V		
	Identity-related information	V		V	V

[12] With the exception of passport information, medical information etc.

However, in the age of ICTs, both general personal privacy information and growing parts of deep personal privacy information are stored in data pools, detached from physical persons. What makes this detachment possible is the ability to translate any category of personal privacy information into bits of 0 and 1. Once detached, the information, in whole or in parts, can be digitally stored across different databases and disseminated through the Internet. In other words, ICTs are allowing us to place any element of personal privacy information in databases and to connect it with other entities, such as information analytics or knowledge in psychology and social sciences. All these tools help make connections between raw data and metadata, giving them meaning. Moreover, associate data with operational tools and derive new data from given information, e.g., derive your preferences based on your shopping data. By consolidating those data, companies can infer market trends based on the preferences of several individual people.

Can John Archibald Wheeler's "it from bit" doctrine, which says that "all things physical are information-theoretic in origin" [21], i.e., that every physical item is at its bottom an information bit that has two possible states – 0 or 1 (true or false), can be applied to personal privacy?

In other words, can the discussion of personal privacy be replaced with a discussion of personal privacy information? The answer is yes, firstly, because each of the basic components of personal privacy carries elements of personal privacy information, which means personal privacy information covers every aspect of personal privacy, and secondly, because personal privacy information meets the GDI requirements for being information and is well-defined based on The Stanford Encyclopedia of Philosophy.

Is information the name of the content that we exchange with the outside world?

In our case, personal privacy information is the content of any discussion of personal privacy. For example, the philosophical discussion of the right to be let alone [22] can be regarded as a discussion of one's right to limit the disclosure of one's personal privacy information, for as Birnhack says in his book, monitoring of individuals using ICTs gnaws at our privacy [23], and what is that "monitoring" but transfer of personal privacy information from the private sphere to the public sphere? Thus, replacing the discussion of personal privacy with the discussion of personal privacy information is justifiable. Gregory Bateson defined the elementary unit of information as "a difference that makes a difference" [24]. In the case of personal privacy, it may mean, for example, the ability to differentiate between people based on different body-related information.

The above ontology of personal privacy information shows that it is an adequate representation of personal privacy because:

- Based on Question 1: Privacy information can be digitized and detached from the individual who the information is subject.
- Based on Question 2: Every physical thing is, at its bottom, a bit of information, and therefore, personal privacy is also essentially personal privacy information.
- Based on Question 3: Any discussion of personal privacy is, in fact, a discussion of personal privacy information.
- Based on Question 4: The personal privacy of individual *X* is differentiated from the personal privacy of individual *Y* at least by their respective privacy information.

These four arguments lead to the conclusion that any discussion of personal privacy can be replaced with a discussion of personal privacy information

The ontology of personal privacy information that we have just seen shows that there is no logical obstacle to such a replacement, or, in other words, to the numeric representation of personal privacy information. The digitization of privacy information is the very thing that allows ICTs to store, process, analyze, and disseminate personal privacy information. Thus, not only is it a well-defined concept, it is also measurable and quantifiable by Claude Shannon's information theory [25]. Some personal privacy information is environmental information, formally defined as "two systems A and B related so that the presence of A as category or state F is associated (correlates) with B, and the presence of B as category or state G can be inferred based on information". In the context of personal privacy, a good example of environmental information is the discovery of one's identity by one's fingerprint. AI technologies make extensive use of environmental information – i.e., signs that are observable in the physical world – to uncover personal privacy information, general and deep alike. One assumption behind such use of AI technologies on environmental information is that there is a valid match between physical items and signs observable in the physical. Another assumption is that we can make valid conclusions about Deep Personal Privacy based on information inferred by AI technologies using statistical adjustment and generalization rules. I am not saying that those adjusted and generalized conclusions are the absolute truth, but I will say that the information and knowledge obtained through adjustment and generalization do apply to specific individual people at a given time and place.

Conclusion

The source concludes that replacing the discussion of personal privacy with a discussion of personal privacy information is justifiable and faces no logical obstacle. This perspective is supported by several arguments: personal privacy information can be digitized and detached from the individual subject, personal privacy is fundamentally viewed as personal privacy information15, and any discussion about personal privacy is, in essence, a discussion about this information1.... Furthermore, individual personal privacy is differentiated by respective personal privacy information15. Because personal privacy information meets the criteria for being information and is a well-defined concept, it is also measurable and quantifiable. The digitization of this information is precisely what allows ICTs to store, process, analyze, and disseminate it.

REFERENCES

1. Oppenheim,Yair Personal Privacy in the Age of the Internet. Spines, 23 Sep. 2024, 46-51
2. Bernardo Periñán, "The Origin of Privacy as a Legal Value: A Reflection on Roman and English Law", *American Journal of Legal History*, vol. 52 (2) (April 2012), 185.
3. Shoshana Zuboff, *The Age of Surveillance Capitalism*

(London: Profile Books, 2019), 8.
4. [4]According to Margaret Rouse, "A smart city is a municipality that uses information and communication technologies to increase operational efficiency, share information with the public, and improve both the quality of government services and citizen welfare". https://www.techtarget.com/iotagenda/definition/smart-city (Accessed April 9, 2024)
5. For more information on cookies, see Benoist, "Collecting Data for the Profiling...", 169-184.
6. Periñán, Bernardo. "The Origin of Privacy as a Legal Value: A Reflection on Roman and English Law". *American Journal of Legal History*, vol. 52 (2) (April 2012): 185
7. Ibid., 186. The author argues this is a violation of privacy that one cannot protect oneself from because the actions in question are performed in the public sphere; to use his expression – "It is like being naked in the village square". I disagree and believe it to be a precise example of the kind of privacy invasion discussed in this book.
8. Lior Rabi, *Omes ha-individualiyut – ha-shorashimshel ideal ha-individualiyut ha-moderni* [The Burden of Individuality: The Origins of the Modern Ideal of Individuality] (in Hebrew) (Haifa: Pardes, 2009), 255.
9. Jorge J. E. Garcia, *Individuality: An Essay on the Foundation of Metaphysics* (New York: State University of New York Press, 1988), 234.
10. Raffaele Rodogno, "Personal Identity Online", *Philosophy and Technology* Vol.25 (3) (2012), 309-328.
11. Marya Schechtman, "Stories, Lives, and Basic Survival: A Refinement and Defense of the Narrative View", in: *Narrative and Understanding Persons*, ed. Daniel Hutto (Cambridge: Cambridge University Press, 2007), 155-178.
12. Marit Hansen and Andreas Pfitzmann, "A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management", 9. https://www.researchgate.net (Accessed 24/1/2021)
13. Michael D. Birnhack, *Merkhav Prati: Ha-zkhut la-pratiyut ha-ishitbeynmishpat le-technologia* [Private Space: The Right to Privacy, Law and Technology] (in Hebrew) (Ramat Gan: Bar-Ilan University, 2010), 286.
14. Kevin Robins and Frank Webster, *Times of the Technoculture: From the Information Society to the Virtual Life* (London: Routledge, 1999), 102-109.
15. Michael D. Birnhack, *Merkhav Prati: Ha-zkhut la-pratiyut ha-ishitbeynmishpat le-technologia* [Private Space: The Right to Privacy, Law and Technology] (in Hebrew) (Ramat Gan: Bar-Ilan University, 284-285.
16. Oppenheim,Yair , Personal Privacy in the Age of the Internet. Spines, 23 Sep 2024, 156-158
17. Luciano Floridi, "Philosophical Conceptions of Information", in: *Formal Theories of Information: From Shannon to Semantic Information Theory and General Concepts of Information*, ed. Giovanni Sommaruga (Springer, 2009), 13-53.
18. Oppenheim, Yair , Personal Privacy in the Age of the Internet. Spines, 23 Sep 2024, 122-135
19. Luciano Floridi, "Philosophical Conceptions of Information", in: *Formal Theories of Information: From Shannon to Semantic Information Theory and General Concepts of Information*, ed. Giovanni Sommaruga (Springer, 2009), 22
20. Stanford Encyclopedia of Philosophy, "Semantic Conceptions of Information", first published Wed 5 Oct, 2005; substantive revision 14 Jan, 2022.
21. John Archibald Wheeler, "Information, Physics, Quantum: The Search for Links", in: *Complexity, Entropy, and the Physics of Information*, ed. Wojciech H. Zurek (CA: Westview Press, 1990), 313.
22. Cayce Myers, Samuel Warren and Louis Brandeis, "The Right to Privacy", 4 Harv. L. Rev 193 (1890), *Communication Law and Policy*, Vol.25 (4) (October 2020), 519-522.
23. Michael D. Birnhack, *Merkhav Prati: Ha-zkhut la-pratiyut ha-ishitbeynmishpat le-technologia* [Private Space: The Right to Privacy, Law and Technology] (in Hebrew) (Ramat Gan: Bar-Ilan University, 35.
24. Gregory Bateson, *Steps to an Ecology of Mind* (New York: Ballantine Books, 1972), 428.
25. Claude E. Shannon, "A Mathematical Theory of Communication",reprinted with corrections from *The Bell System Technical Journal*, Vol. 27 (July, October, 1948):12.

****