Security and Privacy

WILEY

RESEARCH ARTICLE

Exploring Novel Frontiers in Online Privacy Ethics

Doina Gavrilov

Faculty of Political Science, National School of Political and Administrative Studies, Bucharest, Romania

Correspondence: Doina Gavrilov (doina.gavrilov@yahoo.com)

Received: 10 May 2024 | **Revised:** 20 August 2024 | **Accepted:** 28 August 2024

Keywords: personal data | privacy | research ethics | social networks | socialization

ABSTRACT

Social networks have become a new environment in which a large part of our daily life has been transposed. It has become a new research environment and tool for two reasons: It is easy and cheap to use and offers the chance to provide a large amount of novelty. However, questions arise as people navigate privacy on social media differently than in real life, meaning, less intuitively and over a longer time. With this in mind, this study examines how people perceive privacy on social networks and how collecting data without consent violates users' privacy rights, even when the information is public. For this, we focus on the Romanian case study and explore new perspectives on online research to uphold human rights and maintain research objectivity. The results show that managing privacy online is not intuitive, and it requires time for the users to understand how their data can be accessed and used, and to learn the tools they can employ to limit other's access to personal information. We also have found that the majority of our study participants see social networks as a tool for socialization and the use of their information outside this purpose violates their privacy rights. The paper proposes a set of principles and markers to help researchers differentiate between personal and public information to comply with research ethics and not breach human rights.

1 | Introduction

In 2015, Hewson, Vogel, and Laurent [1] explored internet research and emphasized the beneficial impact of internet tools on research endeavors. The first to mention is the researchers' enhanced access to social and minority groups, which were traditionally challenging to locate and engage by using conventional data collection methods. Another positive aspect is the degree of anonymity the internet tools allow users to employ in order to protect their identity. Also, the third aspect is the capacity to reduce people's bias in these new research conditions.

These positive aspects can be guaranteed when the studies are based on questionnaires or online interviews, which involve the tacit information of the research subjects about the method and purpose of data collection. However, what about data crowding, which does not ask for users' consent given that it does not gather identifying information, but the one linked to life experiences, visited destinations, followed groups, people's preferences, etc.? Or in a world where only a few adjust their privacy settings [2], how much do the studies collecting data from the public social networks' profiles comply with the users' data privacy and human rights?

The insertion of social media in our lives has produced some changes by replacing old habits and methods with new ones. We adopted it in our lives so quickly, without considering its impact on personal space, mental health, and human rights. Only by looking at its benefits, we transform it into a tool for socialization, marketing, institutional transparency, and research. Also, in some contexts, we also made it a mandatory tool for learning [3].

In all this context we wonder if people's perception of privacy in social media has changed and if so, we intend to find out to what extent we violate human rights by collecting information from

social media profiles that are accessible and often perceived as public.

1.1 | Study Questions

Trying to understand how privacy is perceived by online users and how online research without user consent for data collection can breach human rights, this study aims to address two key questions: (1) How do people understand online privacy? (2) To what extent does the collection and use of information from social networks without users' consent for purposes beyond socialization violate human rights and research ethics?

1.2 | Research Objectives

To answer the study questions, this paper aims to identify gaps in the current literature and address them by following these objectives:

- O1: highlighting the current definitions of privacy;
- O2: outlining some of the most well-known privacy theories;
- O3: proposing a mixed approach to the concept of privacy;
- O4: distinguishing between privacy in real life and privacy online;
- O5: outlining the online privacy problems by analyzing the sources of privacy rights;
- O6: proposing a set of principles and markers for identifying privacy sources;
- O7: using the Romanian case study to understand how privacy is seen online and to what extent the collection and use of information from social networks represents a violation of the principles of research ethics and human rights.

1.3 | Study Design

To accomplish the study's objectives, we start from the existing literature and approaches to privacy. This helps us understand how privacy is defined and identify the aspects that these definitions overlook in the online environment.

Then, by examining the existing privacy theories, we highlight their limitations and propose a blended perspective on privacy. Specifically, we explore the constructivist theory and a natural approach to explain the authority conflict in online privacy and highlight the origin of privacy rights.

This brings us to a different definition of privacy, one where privacy online is not as natural or intuitive to us as the privacy we exercise and protect in real life. In this new, ever-changing environment, exercising privacy requires specific knowledge of the social networks' tools and of the concepts used in privacy settings to convey the impact of specific changes. Online, privacy boundaries are often pushed by others, and despite our efforts to manage it, the online does not mimic real life, thus exposing our personal information to unwanted individuals.

To address this gap in the protection of human rights, we transfer the ethical and moral responsibility of using social networks' information to the persons accessing and using it.

The rational choice theory puts this responsibility in the hands of the online user sparing the ones that access and use the information without consent. Thus, gives people the difficult task of protecting their personal information and cutting off others' access to it when having limited or no tools for doing that.

But given the circumstances, we pass the moral and ethical responsibility to the ones that access and use others' information, with a special emphasis on the data collection and use by the researchers.

To verify the extent to which our theoretical definition matches the reality and identify other aspects related to online privacy, we focus on the Romanian case study, which is meant to help us understand how users see privacy on social networks, how they manage it, and how aware they are of their data being used without consent, as well as how they feel about it. This helps us identify the extent to which data collection with no consent breaches human rights and affects human dignity.

Additionally, we highlight the internal conflict online users face regarding the use of their personal data in the context of new social trends, what is considered normal, and the need to control all information about themselves, specifically when shared with a particular group of people but used by others with a totally different purpose.

We end the study with recommendations for future research.

2 | Methodology

In our quest towards understanding the impact of social network research on users' data privacy, we follow a mixed methodological approach. Starting from the existing studies we propose a mixed approach to privacy in order to clarify the source of privacy rights and shape a new definition for online privacy. Then, we embrace empirical research to identify aspects of privacy that cannot be easily observed and understood. Therefore, we focus on the Romanian case study and analyze how people perceive online privacy, how they manage it, to whom their information is dedicated, how real is what they post, and how much we breach their rights by collecting data with no consent.

The reason we choose the Romanian case is because of the later introduction of the internet and the social media in the Eastern part of Europe [4] that helps us notice more easily the human accommodation to the social media and its tools, the perception of online privacy, what people consider to be private and how data collection without users' consent affect the human rights and dignity.

For this, we formulated an online anonymous questionnaire with multiple choice and closed-ended questions and addressed it to Romanian online users over the age of 18. The sampling method involves a mix of random and purposive sampling. Meaning, that

the questionnaire was randomly distributed to online users, but only after we selected the accounts that contained basic information indicating they belonged to real individuals. We took this measure to reduce the likelihood of engaging with fake accounts. Thus, we focused on selecting profiles that could be associated with a genuine person.

The questionnaire was built with Google surveys, and disseminated to Romanian online users on Facebook and Instagram. It informed the participants about the purpose of the study, the use of their data, and its anonymous character.

The questionnaire was distributed to 1253 people on Facebook and 82 on Instagram and has a response rate of 8.2%, 111 filled questionnaires.

The analytical sample describes the position and opinion of 53.2% Romanian women and 46.8% men, of which 41.4% are between the ages of 18 and 30, 31.5% between 30 and 40, 18% between 40 and 55, and 9% over 55 years old. The majority of respondents have a higher education degree: 27% hold a bachelor's degree, 36% a master's degree, and 18.9% a doctoral degree. Thus, this study sample reflects the awareness, actions, and perspectives of the educated segment of Romanian society, considering that, in 2023, the year in which the study was conducted, only 16% of the population had a higher education degree [5, 6].

This being said, the study has limitations too, due to insufficient data from the majority segment of the Romanian society, the one without higher education and the seniors. Accessing the ones with no higher education is difficult since often people do not disclose such information on social networks, or use it to lie in their profiles. Also, then, getting in touch with the older ones was challenging too since most Romanian Facebook users are between the ages of 25 and 44 years old, and people over 65 represent only 9.4% of Romanian Facebook users [7].

Additionally, approaching this large group of Romanians was difficult, because most people asked a series of questions before accessing the questionnaire link and required more information to decide whether to participate or not in the study.

Since our study sample primarily consists of individuals with higher education, it reflects the perception of online privacy of those with higher education rather than the Romanian society as a whole.

The collected data is used for comparative analysis and simple statistics to answer the study questions.

3 | Literature Review: The Privacy Meanings

Privacy has its roots in the Latin *privus* which means single. However, the concept can be interpreted differently in various contexts. Privacy alone suggests the individual capacity to isolate from others and preserve personal information from them. In the context of property, privacy points out the individual right and capacity to control their own person, time, and belongings, which together represent symbolically "our autonomy from others and our status as self-sustaining individuals" [8].

Similarly, in 1994 Johnson [9] argued that privacy represents an essential aspect that guarantees our autonomy. However, Moor [10] considered that autonomy does not necessarily require privacy and that it is possible to achieve autonomy with no privacy at all. He referred to daily activities involving data storage, like ordering clothes or food, exchanging money, making calls, etc., which can easily serve as a source of authority conflict, once our data gets stored for a long time. In spite of this, these aspects do not seem to create an authority problem. The reason for this is that our data is normally stored by authorities, structures, and organizations entitled to do so. Thus, we find it normal and build a feeling of trust, especially when the data is used for business activity checks, social safety, and consumer protection. On the other side, many services and activities cannot be done without sharing personal data. Therefore, we accept and do not question the necessity for this since we believe it is for our good.

But the authority subject brings in the concept of privacy because together they imply the individual control over the information about the self. However, having control over the self is a psychological and physical human need, and refers to the individual right and capacity to establish boundaries for others' access to personal information and the right to share it. From here, we identify different perspectives on the privacy concept. Several focus on the individual and define privacy as an individual's necessity and capacity to separate themselves from others, and to "control other's access to the self" [11]. Other authors see the individual as part of society and define privacy as individuals' and groups' capacity to decide when, how, and how much information about themselves can be communicated to others. This approach considers the individual and groups' needs, highlighting their right to withdraw from social surveillance and pressure at any moment they feel doing so [12, 13]. Also, we also have the research focused on the individual and his relationships. Here, the privacy definition varies depending on the degrees of friendship, trust, individual desire to share, etc. In this approach, we find discussions about the inheritance or borrowing the rights to regulate information confidentiality [14, 15].

The, Sidis case and the defended the right to privacy together with the free expression of the press [16], raised the question of privacy limits in the context of social security. Meaning, where should we draw the limits of privacy to offer personal space, but also to guarantee safety?

Trying to answer this question, Hirshleifer [8] argued that privacy cannot be only about secrecy, as Posner sustained in 1978. He stated that privacy is also about "autonomy within society" [8], which, unlike other approaches, highlights not only the individual psychological and physical state towards the surroundings, but also his place, rights, and needs as a member of the society.

These privacy approaches mostly start from the way people behave and exercise their rights in real life. However, issues emerge in the context of social media, where many studies place the responsibility for protecting personal data on the user. However, in an online environment that does not perfectly replicate real life and where maintaining privacy requires ongoing information and tools that don't offer the same control as in real life, to what extent should the responsibility rest only with the account owner?

Most studies on online data privacy focus on empirical findings rather than on proposing a new definition of privacy that would encompass new privacy characteristics in this environment. Often starting from the rational choice theory and focusing on the impact of personal data trade against nonmonetary rewards, a part of the existing studies analyze online privacy and answer several questions at once by passing the decision power and the full responsibility on data privacy to the social media account owner.

The rational choice theory supports the idea that the individual will always choose a solution that involves the smallest expenditure possible in exchange for the achievement of desires. Therefore, starting from the idea that human beings are rational and aware of their choices, researchers argue that the level of disclosure on social media relies on individual needs [17]. Since it is believed that the more is disclosed — the more is achieved. However, this is not always the case. Like in real life, self-disclosure is a precondition for establishing relationships, developing an identity and friendships [18], and it can be psychologically rewarding when leading to a sense of openness-closeness and generating a sense of connectedness and belonging [19, 20]. However, this may work only when disclosure is done selectively and not mandatory, as some situations may require. Even more, it may work if online we could have an environment that could mimic real life in order to manage privacy limits and grant access to our private information to specific individuals for specific purposes. However, as proven, social networks are nothing like real life, and for this reason, the users register different behaviors: While some may be open to sharing, others may be more secretive.

In 2013, Chen [21] studied the impact of personal privacy values and the authority needed on social networks users' privacy preferences. The results showed that social media users "are quite conservative in terms of self-disclosure" in spite of their attachment to networking sites.

Similarly, Forest and Wood [22] showed that individuals with low self-esteem are reluctant to disclose information and build relationships on social networks, despite their ability to manage risks and privacy levels.

We believe that these choices speak of the individual's attention toward the potential long-term impact of online disclosure, like "dislikes of others, harassment or unwanted privacy intrusions" [23–25]. Additionally, users struggle to manage their online privacy as effectively as they do in real life. Posting on social networks and granting access to personal data online cannot be done by looking at the nature of specific situations, only to a specific group of people from our friend list, or for a limited amount of time. On the contrary, it implies opening to a larger group and offering constant access to personal information compared to real life where the individual can easily isolate themself from society and decide when to give others access to information about him and his life experiences.

In this context, Zhang et al. [26] spoke about several types of online privacy that may be disrupted, namely, user's identity anonymity; user's personal space privacy; and user's communication privacy. Due to these vulnerabilities and the previously mentioned aspects, social network users often fall victim to human rights violations, as others exploit their access to personal data, mistakenly assuming that what is accessible is equivalent to being public and can be used freely in various contexts.

In this context, this study aims to address a gap in the field by proposing a definition of online privacy. Starting from this definition, we focus on the moral, ethical, and human rights implications of using information from social networks for research and other purposes without consent.

3.1 | Privacy Theories

In 1967 Westin proposed a theory of privacy, which discussed the individual and group needs and capacity to withdraw from anything involving social pressure and conformation to the social rules while enclosing in a personal space where autonomy and personal information can be preserved. This approach started with three types of social surveillance: Physical, psychological, and data surveillance [13]. The physical and psychological dimensions are linked to our natural behavior and depend directly on present actions, thus, are easier to secure. Meanwhile, data surveillance is not that natural since it involves protecting personal data collected and built by social structures.

When our data is collected by official structures, it is easier to impose rules and control the way this data is used. However, in the new environments of socialization, like social networks, where there is no specific authority and methods to ensure data safety, individuals remain vulnerable to identity theft and other deceptive actions.

Our need for personal autonomy, emotional release, self-evaluation, and controlled communication with others about the self for personal space, have to take place in the absence of social constraints and demands [12, 39], which is vital for individual well-being. However, to fulfill these needs we need privacy, in the sense of our right to decide what to do with our bodies and the information belonging to us. In this regard, Westin [13] argued that there is a serious need for special legislation to protect privacy rights.

Often, Westin's theory was described as individual-centered [27, 28] because of the attention he gave to individual actions, intentions, and needs. However, privacy can also be about collective actions [12], as shown in Altman's approach.

Altman observed that people change their privacy limits and preferences while trying to balance the external conditions and internal states. Hence, the individual tries to regulate interaction with those around them and avoid crowding by constantly setting or removing personal boundaries. The reason for this is maintaining self-identity, which is considered the main purpose of privacy [29]. In this sense, Altman's definition of privacy gives the individual the right to withdraw from social life into a well-defined physical and psychological personal space. For this, Altman spoke about the importance of using body language, eye contact, and physical distance, as mechanisms for establishing and controlling personal boundaries [30]. The knowledge about how to use these mechanisms/techniques of privacy management is the key to our good functioning in society [31].

rivacy online is fundamentally different from privacy in real life. Unlike in the physical world, where individuals can withdraw to isolate themselves from others without causing reactions, the virtual space lacks this simplicity. Additionally, online tools for protecting personal information are not as user-friendly or intuitive as those available in real life. Achieving the desired level of privacy online is not only challenging but also falls short of allowing users to set precise limits for who can access their information. This difficulty in restricting access at various levels leaves us vulnerable, as some may access our data even if we did not intend for it.

But privacy management has a direct impact on the quality of our daily lives: It affects our "safety, security, and physiological needs" [29]. However, our needs differ and privacy is not the same for everyone. Its definitions and limitations constantly vary and adapt to individual life experiences, the external and internal factors.

Starting from this, Kwasny et al. [32] found that males see privacy in terms of convenience and need while females see it in terms of safety and respected privacy rights, and older people see it as something akin to personal space and not to personal information. This difference is drawn by our health status, psychological factors, life experiences, etc.

Considering computer-mediated communication, in 1991 Petronio developed the communication privacy management (CPM) theory, which starts from Altman's perspective on the individual needs to restrict and juggle with privacy limits in order to allow and restrict other's access to the self. Petronio's theory considers that: (a) People believe they own some information and that (b) they have the right to decide to whom and how much they can disclose. (c) People build privacy limits based on culture, gender, motivation, context, risks, and benefits, and they (d) consider that once their private information is shared, the ones that received it become co-owners, and they are, or must be, automatically charged with some responsibility and limits when sharing that information [12, 14].

The CPM theory focuses on the boundaries we establish to isolate ourselves physically and psychologically from social pressure and surveillance. These boundaries are addressed to society with the intention of clearly establishing some rules and limits for individual personal space. With all this, sometimes the boundaries are surpassed and the internal and external states of the individual get affected.

Therefore, to avoid social cross-over personal limits of space and information, Petronio introduced the concepts of boundary-defining ownership, boundary coordination, and boundary turbulence [33]. The first is about a set of limits we use to separate personal information from the one we consider public. We believe this information is ours, and that we have the right to decide to whom, when, and how much we can share. The second is about our capacity to build some safety boundaries for the information we are transmitting. Sometimes we build these boundaries together with the ones the information is shared with in order to create a deeper feeling of privacy and information ownership. Also, the third is about when our boundaries were not effective, and the information we transmitted reaches people it was not intended to reach. This usually happens when co-owners fail to keep our information safe either out of bad intention, by mistake, or because they were under pressure [34].

Both, Petronio and Altman's approach to privacy address individual and group needs together with mechanisms for privacy control. However, we lack a comprehensive definition that differentiates real-life privacy from online one. Thus, we focus next on finding differences between real-life and online manifestation and perception of privacy.

4 | Mixed Approach to Online Privacy: The Real-Life Versus Online Privacy

To understand privacy online in 2011 Ellison analyzed the way communication takes place online and how it influences privacy. In real life, socialization facilitates sharing information to help us survive, develop, and achieve a good level of life. However, social networks developed when most of our basic needs were already fulfilled. Consequently, it entered our lives as a tool for socialization and sharing information about the self [15] rather than as a tool for helping us survive.

In time, social networks were also seen as a communication tool meant to overcome economic crises or pandemics [35], However, mainly they remain an artificial tool for socialization. The reason for this is the level of trust we have in others and how much and how real the information we share in this space is.

In real life, most information we share is verbally or through direct demonstration of abilities, competencies, and characteristics. However, online, information is shared differently, and our level of trust differs starting from the fact that we cannot really know who is behind a profile and their intentions. In social media, as in real life, we are constrained to share personal information to establish connections, to be recognized by specific individuals, to create an identity, and to imitate real-life socialization. However, the ways we manage personal information here are very different from the way we do it in real life.

In real life, we can separate our audience, adopt a specific attitude, and present information in a specific way; we constantly adapt to the audience and their reactions. However, on social media, the audience is usually a group of people from various environments, more or less close to us, and the information we wish to share with relatives can extend to those who are less intimately connected to us.

Also, in real life, our family, close friends, co-workers, schoolmates, university colleagues, school teachers and university professors, club friends, etc. rarely meet. Therefore, the information they have about us is often the one we share and is considered appropriate for those specific contexts. However online, our friends, relatives, colleagues, and others are in a single friends list, and our posts are for all. Thus, the information we post will address all these people, and our online self will most likely never be the same as our real-life self. Probably, most of us will choose a role to play for all, depending on who is the most important from our friends list, and whom we would like

to impress or establish a closer connection with. For this reason, Ellison [15] argued that developing serious relationships on social media is complicated because it implies self-disclosure to a wider audience than in real life.

Another specificity is that online, we communicate information in a visual or audio format, which can be easily disclosed to others, and very hard to move back into our personal space. Unlike real life, where information is usually transmitted verbally and can be easily denied and classified as gossip if it reaches an unwanted public.

Therefore, we realize that the main difference between online and face-to-face privacy lies in the differences between privacy limits and manifestation. However, when privacy is defined as the capacity to remain autonomous from others and be self-sustaining [8], to control other's access to the self [11] and regulate information confidentiality [14, 15], how much of this definition applies to the online environment?

This does not mean that online privacy should differ from that in real life, especially if we start with human needs and human dignity. However, we see that online privacy is different primarily because people look differently at the virtual space than the physical one. With this in mind, we define online privacy as a nonintuitive nor natural practice involving a complex process of learning new tools and concepts of social networks to manage others' access to personal information.

4.1 | Questioning the Source of Privacy

The way we live and how society is organized nowadays makes it impossible to be totally separated from others. Although we may want moments of total solitude, social interaction is crucial for accumulating information about the world and ourselves. As Vazire and Carlson [36] showed, sometimes, others know us better than we do, because our ambitions, desires, filters, and beliefs shape the way we see ourselves. Therefore, we socialize to exchange information, negotiate, give meaning, and verify our knowledge [37].

However, most of the information we have about ourselves is collected or built by society. For example, our name was given to us by our parents, the phone number was given to us by the phone company and associated with our name, the general information about ourselves like, how beautiful, smart, tall and funny we are, is built by considering the social concepts of beauty, smart, and funny and by comparison with others. Therefore, when most of the things we know come from society, and what we find about ourselves is a result of self-evaluation through social concepts, we wonder if this information ever belonged to us. Also, what is to be considered personal information?

If "we are shaped by culture, and culture shapes who we are" [38] and if integration, as a process of adaptation by learning new skills, behaviors, and rules, "expands our sense of who we are" [38], then who we are is nothing but a result of social work — the work of our parents, teachers, relatives, friends, and everyone we interact with, that contributed to our development and to discovering ourselves.

But, if our identity, our person, and our character are to be the result of our interaction with society and society's work, then how entitled are we to control this information that never belongs to us, that we just embraced in our journey towards understanding and finding ourselves?

With this in mind, we wonder what is that "something" that gives us the right to control some information related to ourselves. In addition, where does privacy spring from?

4.2 | Source of Privacy Rights

In 1992, Bezanson mentioned that the press was seen as a threat to the individual identity even since 1890, because of the social fear of press transforming identity from an individual construct into a social construct. However, the press was only a tool for disseminating social reality models, principles, and ideas when societies have always built and influenced everything through communication and socialization [37]. Since we are born, we learn to do things the way everybody does, think in terms of good and bad defined by society, follow social trends, and seek to integrate in order to benefit from belonging to society, etc.

Therefore, we are social constructs. We have a culture, traditions, ways of thinking, a name, a unique identification number, etc. we receive and learn from society. Most of the things we know about ourselves would have no meaning if disclosed to somebody outside our society and culture. In other civilizations and cultures, we may be ugly, silly, and weak, while in the society we grew up in, we may be beautiful, smart, and strong. It is all about how society defines everything.

This social constructionist approach partially explains the issue of privacy but does not align with contemporary human rights perspectives, from where the authority conflict arises and the right for data privacy springs. One of the questions to clarify this subject is: Would the information about the individual exist without him? The answer to this question moves back to the individual his rights to manage certain information.

However, interested in what kind of information is to be considered private and requires user consent, at first, we look at the source of information and the reason why the individual associates some information with themself. In this light, we propose four principles to help researchers identify private information:

1. The existence principle: It questions whether the information would have existed without the individual. Meaning, that the information does not belong to the individual if it could have existed, or been built, without him.
2. The isolation principle: There is information that can be understood, perceived, and used outside any society, like hair, eye and skin color, fingerprints and iris shape, height, physical skills or disabilities, the degree of irritability, the way of reacting to certain external and internal factors, etc. This information belongs to the individual from the moment it builds an image of someone and is directly associated with a person describing unique features of body and personality.

3. The provenience principle: Information has two major sources: Either it is accumulated through the human senses (sight, hearing, smell, and touch), or it is accumulated through communication. When information about the individual is accumulated by observing the individual, then this information belongs to him. Some information can be constructed by interaction with social constructs, such as religion, the political preferences. However, the information belongs to the individual as long as it is primarily built through observation and interaction with the individual. In this case, the information belongs also to the person that has built it.
4. The uniqueness principle: One of the biggest differences between individuals is their life experience, the historical period they lived in, and many other factors that influenced their development. The information we build by interacting with the surroundings also belongs to us, because it was built through our decisions and actions.

Also, there are the simple and basic aspects that make us different, namely, the ones we were born with (fingerprints, DNA, iris shape), and the more or less unique ones that were given to us at birth or acquired through life (name and first name, unique identification code, scars, etc.)—all this information belongs to us.

Following the uniqueness principle, we identify a set of markers highlighting our right to consider some information personal and to manage it. For example, we have:

1. The biological markers—the physical aspects that distinguish us from each other and make us unique, like DNA, iris shape, and fingerprints.
2. The cognitive markers. Starting from our life experiences, physical condition, and the environment in which we grew up, each of us gets to accumulate a certain set of information. Based on this, we will judge things in a certain light and will behave accordingly.
3. The psychological markers. Here we have the aspects outlining our character. One of the most important are the definitions of good and bad that we internalize, the associations of something with good, bad, weak, strong, or normal, the lessons we learned through life, and the personal principles we have built to guide our decisions and behavior. To this, we add the culture, religion, and traditions, which have a huge impact on our psychological markers that shape our judgment and behavior each step of the way.
4. The emotional markers. Emotional markers are the information deriving from personal experience that had a major impact on our emotional state. All the fears and joys that we experienced, and the circumstances we were in mark us in a unique way and leave a special imprint on our behavior. The emotional markers serve as triggers of certain fight or flight states, or as motivators for our daily actions.

All these markers can be considered levers for identifying and classifying personal information. These principles and markers are meant to help researchers and online users differentiate between private and public information.

A simple disconnection from social networks does not allow the individual to completely isolate themself because their information remains exposed, and the online self does not have "breaks." The moment we disconnect from social networks, we remain active for the ones who want to send us messages, comment on our posts, or know more about us from our profile. In real life, however, from the moment we enter the house, society no longer has access to us unless we want it. This is how online privacy is more like a technical construct meant to imitate real-life privacy and allow individuals to protect their rights.

5 | New Perspectives on Online Privacy: A Romanian Case Study

Any information that resides from us, or to the construction of which we contributed, is considered personal. It serves as a key to knowing us and the culture we belong to, and because of this, it has always been protected. Personal information can be used in a good sense, to identify what we have in common with others to communicate easier, but it can also be used in a bad way to disintegrate someone's image and cause irreversible harm.

Privacy limits have always been pushed by society, which is in a permanent search for entertainment and information to redefine safety and correct behaviors that deviate from social norms. However, the insertion of social networks in our daily lives made it even harder to manage privacy, since online we have a totally new environment where we differentiate between "contextual, relational, performative and dialectical" privacy and need different tools to settle privacy boundaries for others [39]. These boundaries vary from one person to another and from one situation to another depending on our "individual preferences, abilities, and context-dependent social meanings" [39].

Intending to find out how privacy is seen in the online environment, what information is considered private and what is not, the extent to which people want to protect their information, the ease of adjusting privacy settings, and the difference in information sharing online versus real life, as well as how these aspects influence human rights, we focused on the Romanian case study.

5.1 | Study Findings

In our quest towards understanding privacy, we focused on the Romanian case to study the users' perception of online privacy. 95.5% of our respondents have a Facebook account, 80% have an Instagram account, 34.5% have a TikTok account, 30% have a Twitter account, and 29.1% have an account on other platforms and use specific applications for socialization. The amount of time spent on these platforms is different (see Figure 1).

However, the reasons our respondents use social networks also vary. Most people use them for getting informed on different topics (87.3%), socializing with friends and relatives (77.3%), maintaining friendships and connecting with different people (50.9%), and knowing better political personalities (24.5%). In

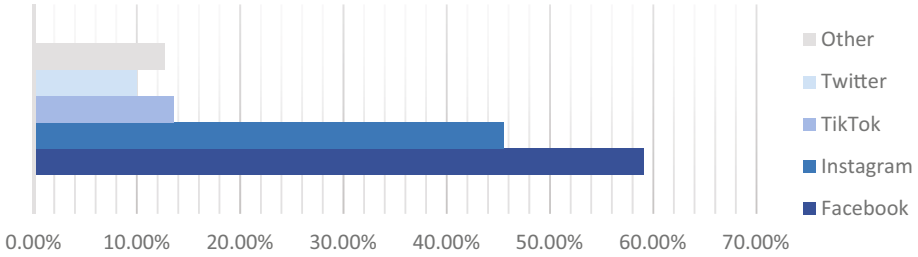

FIGURE 1 | Time spent by Romanians on social networks. *Source:* Author's figure.

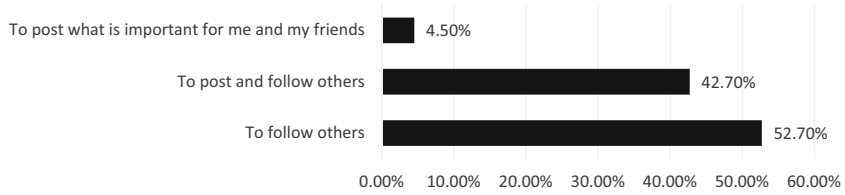

FIGURE 2 | Motivations behind social network usage. *Source:* Author's figure.

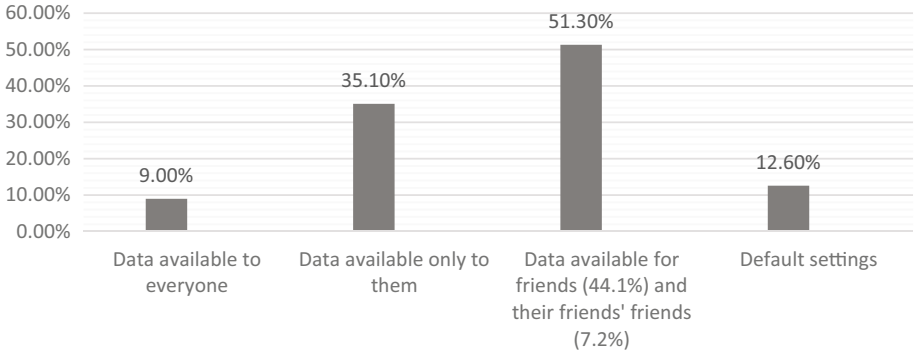

FIGURE 3 | Data settings management on Facebook. *Source:* Author's figure.

line with this, we find out that most of our respondents are first of all consumers of information and occasionally content creators (see Figure 2).

This shows us that social networks are primarily seen as a source of information for society and only then as a space where meanings, ideas, values, and social principles can be shared and negotiated.

Social networks are mostly seen as a space for socialization but not as an official page for displaying personal valid information. It is rather a tool for getting informed and creating and maintaining relationships, which automatically implies disclosure. However, this does not mean that the shared information is complete, valid, and updated. Also, even when shared, the information is directed to family and friends and rarely to strangers.

When we define personal information as the information about the self which includes the name, surname, date, and place of birth, phone number, email address, current and past jobs, pictures with family, and daily life aspects, we observe the reluctance of our respondents towards sharing it on social media. By asking about their settings' choice on the visibility of this data on social networks, we see that one-third of the respondents preferred to keep this data for themselves, and 44.1% made it available only to their friends (see Figure 3).

This shows the majority's preference to keep the information they consider to be personal or private for themselves and the ones from the friend list. In spite of this, there is information that our participants do not necessarily consider to be private, like their posts about something else than themselves. In this case, the preferences vary. For example, when it comes to the information about the likes, shares, or comments of the users on pages and posts about various products, sales or promotions, news, etc., 24.3% of our respondents do not consider this information to be personal and 43.2% have it visible to anyone. However, when asked if they would modify the settings in this direction, 23.6% said they would check the settings again to modify them, while 43.6% set up their settings a long time ago, and only 32.7% did not mind sharing this kind of information.

This shows us that people believe the settings they selected long ago will remain in place and be updated, even when privacy settings change and become more detailed on social networks. In spite of this when it comes to data collection for social networks, 76.6% of our respondents prefer for their consent to be asked if the information from their profile is to be used for anything else

than verifying their identity. Only 12.6% do not have any preferences or problems with the information from their profile being collected without their consent.

This turns us towards the controversial question: If the information is public why cannot it be used?

This is where we recognize the common mistake online users make by confusing accessible information with public information. The difficulty users face in keeping up with changes on social network platforms, adapting to privacy management tools, and bearing the sole responsibility for managing their private information seems unfair, especially given the lack of accountability for those who collect data without consent. This is where we believe that the responsibility for protecting personal data and human rights falls within the hands of all the actors: The account owners but also the ones that collect and use information from social networks without user consent.

A solution to raise the social awareness on the necessity to constantly adjust their privacy settings for data privacy can be done through information campaigns. However, such actions would require special resources and lots of time. That is why, for now, informing the social networks' users on data privacy settings remains an informative necessary action of most platforms. Still, not too many users try to change data privacy settings [2] given that people have different methods of learning and may need special explanations, that privacy itself is a complex construct requiring lots of effort for understanding, and that individuals' interest may be raised only when pointing directly how something can affect them. In this light, the task of protecting personal data and not breaching the human rights when conducting research remains in the hands of the researchers.

One of the reasons why the accessible data is not necessarily public is because of the way people see social networks. Their privacy settings may grant access to everybody's personal data and the user's posts, but the intended audience was different than the one. In our case, of the ones that post on social networks, 42% address the posts to their family, close friends, and friends, and not to strangers (see Figure 4). This is where the authority conflict arises: When managing the privacy settings is not that intuitive and natural, and the information we post is used without considering the individual preferences and the intended public.

This is where we highlight the ethical nonconformities of a study with data collected without user consent. Such a study would

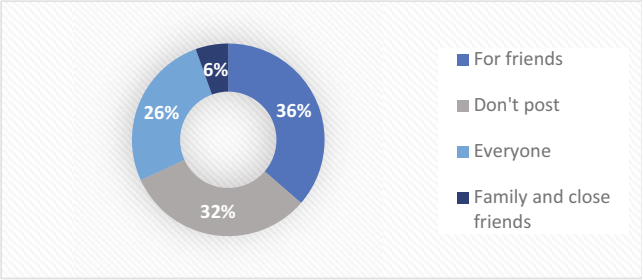

FIGURE 4 | Posts on Facebook and their intended audience. *Source:* Author's figure.

mean breaching the Article 8 of the European Convention on Human Rights (ECHR) on Equality and family rights [40]. This means that the right to build friendships, an identity, and other relationships could be violated in the context where collecting data about the individual or his preferences without consent can lead to restrictive policies or actions that would affect private and family life.

This would also lead to the violation of the general data protection regulation (GDPR) of the EU. However, the breach of these regulations and the ECHR can be unclear when the collected data is about counting the number of people on the social networks who appreciate, buy, or own specific products, their travel destinations, income estimations, and other aspects since they do not focus on the individual and do not intend to directly affect him. Still, these data points could lead to policies with impact on the individuals from whom the data was collected and affect their identities, relationships, family life, etc.

In line with this, we highlight the importance of returning to this paper privacy principles and markers for identifying private information. Meaning, that even though researchers do not intend to build individual profiles or collect personal data in the traditional form, the necessity for asking for the users' consent comes from the existence and the provenience principles. In this sense, the collected data is personal because it would not exist without the individual's actions and participation online. The individual character and life experience of users led to their specific preferences, and their online involvement and participation made our data collection possible.

With this in mind, we turn towards Romanian's openness to being approached by strangers and we see that 58.2% of our respondents offer to anyone the possibility to send them a friend request, 21.8% of the respondents were not interested in this aspect and left the settings as they were set up initially, and only 20% prefer to know how a new person found them, so they allow the invites to be addressed only by their friends' friends.

This highlights that although people are protective and reluctant to communicate with strangers, they do not want to eliminate the possibility of being contacted by others. However, what about using the data for advertisement dissemination, communicating it to partners, or the elaboration of market and impact studies based on it? In this matter, 86.4% of our respondents are aware of their data being collected by Facebook and shared with third parties, and 66.4% of them are bothered more or less by this. However, when asked if they would agree for their data to be collected by the state institutions for the development of feasibility and impact studies or for building social policies, 55% answered that they would not agree for their data to be collected by state institutions. Only 19.8% agree in this matter, and 25.2% do not have preferences in this direction since they believe that the collection of personal data by the state institutions from their social networks' profiles would not affect their personal life.

Quite important though, 85.6% of our respondents consider the information from their social networks page belonging to them and would prefer for their consent to be asked if their data is to be used for anything else than socializing, but the preferences

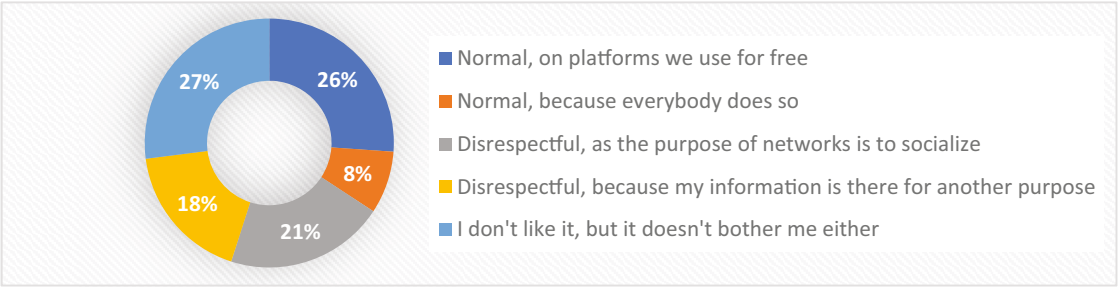

FIGURE 5 | Romanians' attitude towards using social network data for marketing strategies, research, and product/service sales. *Source:* Author's figure.

change in the context of the "new normal." 26.1% consider it normal for companies, firms, researchers and institutions to use their personal information for studies, designing marketing strategies, etc. since the use of social networks does not require any payment. Also, 8.1% consider it normal for their data to be accessed by various structures and individuals online since everybody does so (see Figure 5).

We observe a clash between the "new normal," where easy access to personal information makes it normal to use it for purposes other than socializing, and the "old normal," which emphasizes the individual desire to control other's access to personal information. In this light, in spite of what people consider to be normal, 39% of our respondents consider that using their personal data with no consent for studies and other purposes except knowing them proves a lack of respect, affecting their dignity, authority, and rights to control personal information since that information is there with other purposes. Not only this, but 76.6% of our respondents prefer to be asked for consent if their personal data is to be used for something other than verifying their identity.

In this case, if their consent were asked, 31.8% would agree for their personal data to be collected by state institutions for impact studies, 34.5% would agree for their information to be collected by advertising agencies, and 12.7% consider that their personal information can be collected by anyone to whom they give consent.

6 | Discussion

This study has found that the educated segment of Romanian society sees social networks as tools for socialization and as a source of information. Thus, any use of their information outside these purposes initiates an authority conflict on data privacy.

The majority of our respondents are aware of the fact that their online activity is monitored (by Facebook, for example) and that their information can be collected and later used for impact studies, marketing strategies, etc. In this light, several respondents consider it normal to collect their data with no consent from social networks since everybody does so, and especially when social networks provide free services. However, collecting data without consent is not approved by 85.5% of our respondents and represents a violation of human dignity, an action against authority and individual rights to control personal information.

As the online environment forces us to disclose more personal information so that socialization can take place with a sense of trust among the participants in the discussion, it is necessary for researchers to take into account the way social networks are seen, to whom personal information and posts are intended, and the need to differentiate accessible information from the public one.

In this sense, the questionnaire shows the people's wish for their data privacy rights to be respected while constantly exposing some information for maintaining and initiating relationships and friendships. This highlights users' difficulty in achieving their desired level of data privacy online due to several factors: Limited platform settings, challenges in keeping up with changes on social networks, lack of knowledge about behind-the-scenes actions, social pressure to share more information, the need to lower privacy barriers for communication, the unique nature of the online environment, and the challenge of behaving naturally within it.

This is how privacy on social networks often becomes an illusion, a mental construct where people believe their information will be used only by those it was intended for, not by others. This illusion is rooted in people's common sense and hopes that ethical and moral principles will be respected. Therefore, researchers must consider the intended audience and privacy principles when deciding whether to seek consent before collecting data.

Online, people share more personal information to simulate real-life interactions. However, they cannot easily limit access to specific groups within their friends list due to the limited tools for categorizing friends and setting different privacy levels. Only recently has Instagram introduced the "close friends" option for stories, allowing users to share content with a specific group for a limited amount of time.

When people view social networks primarily as communication tools, they often do not question the use of their data for other purposes, particularly since they are not directly involved in the research environment and may not be aware of such activities or their potential impact on daily life. As a result, using information from social networks without users' consent creates a conflict of authority and violates their rights to control and share personal data.

7 | Conclusions

Starting from the disparities in social interaction between online and face-to-face contexts, this study aimed to propose a new definition for online privacy and uncover other aspects of it from the Romanian case study.

Starting from the existing research and definitions of privacy we highlighted that online privacy is different than real life in the sense that if real-life privacy is about the human capacity to manage other's access to the self, then online privacy is about a complex process of learning new tools and concepts of privacy and confidentiality and juggling with a constantly changing set of privacy settings to protect personal data.

With this in mind, we focused on the Romanian case study to explore additional aspects of online privacy and the ethics of using accessible data for research without user consent. The study has shown an internal conflict between the users in the context of the new normal and the old privacy principles. This highlighted users' desire to achieve a high level of privacy online considering that they mostly use social networks to connect with others, speak, and gather information about daily life but not for other purposes. In this direction, researchers must also consider the social media trends and the lack of specific tools to verify the truthfulness of information that people use to post "privacy lies" [41], which raises a serious question mark on the objectivity of studies.

Finally, the study highlights the users' perception of online privacy, their internal conflicts, and the opposing opinions, underlying the other's ethical and moral responsibility to ask for consent when collecting and using data from social networks for something else than socializing and verifying someone's identity.

In this direction, we proposed a set of principles and markers to help researchers differentiate personal information from the public one when conducting a study.

This paper aimed to contribute to security, privacy studies, and research ethics by highlighting how social network users perceive privacy and how data collection without their consent breaches human rights and research ethics. Additionally, it opens new avenues for privacy research in related fields. It raises questions for human rights researchers to examine the extent of rights violations when individuals either do not change privacy settings or consciously use social networks solely for socializing.

It also presents challenges and questions for researchers and IT practitioners, urging them to develop programs that simulate social environments and provide tools to better mimic real-life privacy online.

This study also raises questions for philosophical discussions on privacy, considering the constantly changing data privacy settings, varying social network platforms, and the common person's difficulty in understanding abstract concepts and their impact on daily life.

Lastly, the study highlights the internal conflict individuals face between accepting the "new normal" and their right to control personal information. This issue could serve as a basis for privacy and confidentiality studies, aiming to identify the privacy boundaries in a contemporary, globalized society.

Data Availability Statement

The data that support the findings of this study are openly available in Figshare at https://figshare.com/articles/dataset/Research_data_for_Exploring_novel_frontiers_in_online_privacy_ethics_/26520745, reference number https://doi.org/10.6084/m9.figshare.26520745.v1.

References

1. C. Hewson, C. Vogel, and D. Laurent, *Internet Research Methods* (London, UK: SAGE, 2015).

2. R. Gross and A. Acquisti, "Information Revelation and Privacy in Online Social Networks," in *Workshop on Privacy in the Electronic Society* (Alexandria, Virginia, USA: Association for Computing Machinery, 2005), http://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=a7f7397c64a9e610d0f1e55fa653dba257bef442.

3. C. Greenhow and C. Lewin, "Social Media and Education: Reconceptualizing the Boundaries of Formal and Informal Learning," *Learning, Media and Technology* 41, no. 1 (2015): 1–25.

4. A. Sas, "Internet Usage in Central and Eastern Europe – Statistics & Facts," 2023, https://www.statista.com/topics/8298/internet-usage-in-cee/.

5. Euronews, "România, Codașă în UE la Absolvenții de Universități. În Tara Noastră Sapte din Opt Regiuni de Dezvoltare au Procente sub 25%," 2023, https://www.euronews.ro/articole/romania-codasa-in-ue-la-absolventii-de-universitati-in-tara-noastra-sapte-din-opt.

6. M. Pop, "Procentul Românilor cu Studii Superioare a Crescut Simbolic în Ultimii Cinci Ani/Creștere Ușor Mai Pronunțată în București, în Timp ce în Unele Regiuni Procentul a Scăzut," 2023, https://www.edupedu.ro/procentul-romanilor-cu-studii-superioare-a-crescut-simbolic-in-ultimii-cinci-ani-crestere-usor-mai-pronuntata-in-bucuresti-in-timp-ce-unele-regiuni-procentul-a-scazut/.

7. Statista Research Department, "Facebook User Distribution in Romania 2024, by Age Group," 2024. https://www.statista.com/statistics/1178591/romania-share-of-facebook-users-by-age/.

8. J. Hirshleifer, "Privacy: Its Origin, Function, and Future," *Journal of Legal Studies* 9, no. 4 (1980): 649–664.

9. D. Johnson, *Computer Ethics*, 2nd ed. (Englewood Cliffs, NJ: Prentice Hall, Inc, 1994).

10. J. Moore, "Towards a Theory of Privacy in the Information Age," *ACM Sigcas Computers and Society* 27 (1997): 27–32.

11. I. Altman, *The Environment and Social Behaviour: Privacy, Personal Space, Territory Crowding* (Monterey: Brooks/Cole, 1975).

12. S. Margulis, "The Three Theories of Privacy: An Overview," in *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web*, eds. S. Trepte and L. Reinecke (Berlin/Heidelberg, Germany: Springer-Velarg, 2011), 9–17.

13. A. Westin, *Privacy and Freedom* (New York: Atheneum, 1967).

14. S. Petronio, *Boundaries of Privacy: Dialectics of Disclosure* (New York: State University of New York Press, 2002).

15. N. Ellison, "Negotiating Privacy Concerns and Social Capital Needs in a Social Media Environment," in *Privacy Online*, eds. S. Trepte and L. Reinecke (Berlin: Springer, Heidelberg, 2011).

16. S. Barbas, "The Sidis Case and the Origins of Modern Privacy Law," *Columbia Journal of Law & the Arts* 21 (2012): 21–69.

17. S. Kumar, K. Saravanakumar, and K. Deepa, "On Privacy and Security in Social Media – A Comprehensive Study," *Procedia Computer Science* 78 (2016): 114–119.

18. N. Kramer and J. Schawel, "Mastering the Challenge of Balancing Self-Disclosure and Privacy in Social Media," *Current Opinion in Psychology* 31 (2020): 67–71.

19. D. Tamir and J. Mitchell, "Disclosing Information about the Self is Intrinsically Rewarding," *Proceedings of the National Academy of Science USA* 109, no. 21 (2012): 8038–8043.

20. N. Bazarova and C. H. Yoon, "Self-Disclosure in Social Media: Extending the Functional Approach to Disclosure Motivations and Characteristics on Social Network Sites," *Journal of Communication* 64 (2014): 1–23.

21. R. Chen, "Living a Private Life in Public Networks: An Exploration of Self-Disclosure," *Decision Support Systems* 55, no. 3 (2013): 661–668.

22. A. Forest and J. Wood, "When Social Networking Is Not Working: Individuals With Low Self-Esteem Recognize but Do Not Reap the Benefits of Self-Disclosure on Facebook," *Psychological Science* 23, no. 3 (2012): 295–302.

23. N. Aharony, "Relationships among Attachment Theory, Social Capital Perspectives, Personality Characteristics, and Facebook Self-Disclosure," *Aslib Journal of Information Management* 68, no. 3 (2016): 362–386.

24. M. Walrave, I. Vanwesenbeeck, and W. Heirman, "Connecting and Protecting? Comparing Predictors of Self-Disclosure and Privacy Settings use between Adolescents and Adults," *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 6, no. 1 (2012), https://doi.org/10.5817/CP2012-1-3.

25. S. Ostendorf, Y. Meier, and M. Brand, "Self-Disclosure on Social Networks: More Than a Rational Decision-Making Process," *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 16, no. 4 (2022): 2, https://doi.org/10.5817/CP2022-4-2.

26. C. Zhang, J. Sun, X. Zhu, and Y. Fang, "Privacy and Security for Online Social Networks: Challenges and Opportunities," *IEEE Network* 24 (2010): 13–18.

27. A. Westin, "Privacy and Freedom," *Washington and Lee Law Review* 25, no. 1 (1968): 166–170.

28. S. Margulis, "Privacy as a Social Issue and Behavioural Concept," *Journal of Social Issues* 59, no. 2 (2003): 243–261.

29. V. Kupritz, "Privacy Management at Work: A Conceptual Model," *Journal of Architectural and Planning Research* 17, no. 1 (2000): 47–63.

30. P. Wisniewski and X. Page, "Privacy Theories and Frameworks," in *Modern Socio-Technical Perspectives on Privacy*, eds. B. P. Knijnenburg, X. Page, P. Wisniewski, H. R. Lipford, N. Proferes, and J. Romano (Cham, Switzerland: Springer, 2022), 15–41.

31. C. Weber, B. Gatersleben, B. Degenhardt, and L. Windlinger, "Privacy Regulation Theory," in *A Handbook of Theories on Designing Alignment Between People and the Office Environment*, eds. R. Appel-Meulenbroek and V. Danivska (London: Routledge, 2021), 68–81.

32. M. Kwasny, K. E. Caine, W. A. Rogers, and A. D. Fisk, "Privacy and Technology: Folk Definitions and Perspectives," *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* 2008 (2008): 3291–3296, https://doi.org/10.1145/1358628.1358846.

33. S. Petronio and W. Durham, "Communication Privacy Management Theory," in *The International Encyclopaedia of Interpersonal Communication*, eds. S. Petronio and W. Durham (London: SAGE Publications, 2015), 335–347.

34. C. Kennedy-Lightsey, M. M. Martin, M. Thompson, K. L. Himes, and B. Z. Clingerman, "Communication Privacy Management Theory: Exploring Coordination and Ownership between Friends," *Communication Quarterly* 60, no. 5 (2012): 665–680.

35. D. Gavrilov, "Internet Research Tools and Methods – A Continuous Challenge in the Activity of the Ethics and Deontology Commissions," *Etică și Deontologie* 2, no. 1 (2022): 73–84.

36. S. Vazire and E. Carlson, "Others Sometimes Know Us Better Than We Know Ourselves," *Current Directions in Psychological Science* 20, no. 2 (2011): 104–108.

37. P. Berger and T. Luckmann, *The Social Construction of Reality* (London, UK/New York: Penguin Books, 1966).

38. D. Siegel, *The Developing Mind: How Relationships and the Brain Interact to Shape Who We Are*, 2nd ed. (New York/London, UK: Guilford Press, 2012).

39. V. Steeves and P. Regan, "Young People Online and the Social Value of Privacy," *Journal of Information, Communication and Ethics in Society* 12, no. 4 (2014): 298–313.

40. Equality and Human Rights Commission, "Article 8: Respect for Your Private and Family Life," 2021, https://www.equalityhumanrights.com/human-rights/human-rights-act/article-8-respect-your-private-and-family-life.

41. S. Shruti, N. N. Bazarova, and D. Cosley, "Privacy Lies: Understanding How, When, and Why People Lie to Protect Their Privacy in Multiple Online Contexts," in *2018 CHI Conference on Human Factors in Computing Systems* (Montreal, Canada: CHI, 2018).