Jan 17th, 12:00 AM

Understanding Cyberprivacy: Context, Concept, and Issues

Bahaa Eltahawy
University of Vaasa, bahaa.eltahawy@univaasa.fi

Duong Dang
University of Vaasa, duong.dang@univaasa.fi

Understanding Cyberprivacy: Context, Concept, and Issues

Bahaa Eltahawy[1], Duong Dang[1]

[1] University of Vaasa, School of Technology and Innovations, Vaasa, Finland
{bahaa.eltahawy,duong.dang}@uwasa.fi

Abstract. Cyberprivacy has become one of the most worrisome issues in the age of digitalization, as data breaches have increased at an alarming rate, and the development of technology has changed privacy norms themselves. Thus, maintaining cyberprivacy is important for both academia and practitioners. However, the literature on cyberprivacy is fragmented, since the topic is multidisciplinary and often confused with cybersecurity and data privacy. In this study, we seek to understand cyberprivacy by conducting a comprehensive literature review and analyzing 79 selected articles on the topic between 2008 and 2021. Our analysis shows that there are eight contexts associated with cyberprivacy. We proposed concepts on cyberprivacy from different views and highlighted four issues related to cyberprivacy for future consideration. Taken together, the knowledge on cyberprivacy, its challenges and its practices does not seem to accumulate. Consequently, there is a need for more targeted research on the topic to cover different contexts.

Keywords: Cyberprivacy, Cyberspace, Cybersecurity, Literature Review

1 Introduction

Rapid information technology communications (ITC) advances have brought changes to values, norms, and privacy. For instance, individuals would choose to share their right to be unobserved [1] for services and other benefits [2]; yet, service providers and third parties would use monitoring technologies [3] to collect more data than allowed and agreed upon. Traditionally, computer security (COMPUSEC) and information security (InfoSec) measures [4] are used to protect individuals and systems from malicious activities. Three perspectives of protection are often considered, including confidentiality, integrity, and availability (CIA triad). However, although COMPUSEC and InfoSec target these issues, they have a narrow scope and limited practices as they only deal with confined and isolated systems [4]. With the involvement of the Internet, computing devices taking different forms, and the unprecedented proliferation of data, it is thus very difficult to cope with privacy in cyberspace, i.e. cyberprivacy in a digital environment [5]. This is because of the blurring between the individual as a physical organism with its own rights against digital identity and its capabilities [7, 8, 9] and cyberization [6]. As a result, it is argued that protection must go beyond traditional measures.

17th International Conference on Wirtschaftsinformatik,
February 2022, Nürnberg, Germany

Despite the importance of protecting digital identity rights and privacy, there is no general agreement on the exact scope of the term privacy [5]. In a similar vein, even though cyberprivacy is discussed in previous literature [10, 11, 12], there is a lack of a common understanding on cyberprivacy in terms of scopes, issues and context. Hence, in this study, we tried to address the topic of cyberprivacy and build an adequate understanding of it - which helps to improve protection of individuals, systems, and institutions in cyberspace - by answering the following research question: What is the context, concept and issues of cyberprivacy discussed in the literature? By answering this question, we determine the meaning of cyberprivacy in existing contexts, provide clear definitions of the key concepts of the topic, highlight the change that led to this issue, and in consequence emphasize on the actions needed to address it.

In the following sections background is presented (Section 2), followed by the methods (Section 3). Section 4 presents the findings, while Section 5 illustrates discussions. Finally, conclusions are drawn in Section 6.

2 Background

The "Right to Privacy" has been highlighted as a fundamental right since the early Harvard Law Review of 1890 [13]. Nowadays, this right has become one of the most complex issues to address [14, 15, 16] due to the paradoxical views and interpretations in dealing with personally identifiable information (PII) [17] of different stakeholders, such as the legislative perspective, the technical side, the commercial side, and the government side. According to [2], the dilemma of privacy arises from the benefits and transparency resulting from the use of data against the concerns of misusing sensitive personal information. With the help of [18] and [19], it is clear the need for dedicated privacy research that combines technical, human and social sciences, thus to address and understand implications of privacy to maintain trust, draw on what is or is not technically achievable, and suggest the right direction for privacy solutions.

There are two concepts related to cyberprivacy, namely, cyberspace and cybersecurity. First, cyberspace was considered as one of the most confusing terms in science over the past decade as the boundaries no longer exist, and the interaction is fast-paced with no control of any kind [20, 21]. According to [22], cyberspace refers to "the global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" [23]. Domains of cyberspace is, but not limited to the Internet; Internet-of-Things (IoT) technologies; Communication and Mobile technologies; Cloud Computing; data sciences and applications of Big Data (BD), Machine Learning (ML), Deep Learning (DL), Data Mining (DM), and Artificial Intelligence (AI); Blockchain; Virtual Reality (VR) and Augmented Reality (AR); Information Technology; Operational Technology (OT); and the human factor on top [22, 23].

Second, cybersecurity is defined as "the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights" [24]. In [25], the

National Institute of Standards and Technology (NIST) defined three domains for protection, i.e. people, technology, and processes. NIST also provided detailed guidelines on the given domains and could provide adequate protection against most of the current issues. However, despite the existence of these guidelines, the issue is beyond typical security measures of cybersecurity. For example, PII associated with data, and the potential risks is one of the issues [17]. Another example is the issue related to traceability of involved parties [26], by connecting-the-dots [27, 28, 29] and similar mechanisms.

To our best knowledge, there is no common understanding of cyberprivacy, but rather mixed ones of cybersecurity, Internet and data privacy. However, cyberprivacy in our opinion, is a unique concept that addresses the issue of protection from a holistic perspective including security, persona, and legislative matters. Unfortunately, literature on these issues is scarce. Thus, we tried here to cover these topics and related ones, in favor of understanding the context, concept, and issues of cyberprivacy.

3 Methods

3.1 Methodology

The systematic research methodology practices of Okoli and Schabram [30] were adopted and followed by the recommendations given by Schryen [31], and Rowe [32]. As we consider cyberprivacy as privacy in cyberspace [33], we built our knowledge by searching articles in Information Systems (IS) and related disciplines. We searched in the specialized database Finna[1], and then in IEEEXplore and Google Scholar. Regarding search terms, searching the terms 'Cyber' and 'Privacy' was misleading as it returned results related to either privacy in general or cyber-related topics. Accordingly, we searched the term 'Cyberprivacy' and all combinations of its parent term 'Cyber Privacy'. The search yielded 191 and 1490 results for 'Cyberprivacy' and 'Cyber Privacy', respectively. We analyzed the term 'Cyberprivacy' and the term 'Cyber Privacy', articles were then categorized by year. From this initial analysis, the year 2008 was set as the lower limit of this study (four articles exempted from this criterion due to their importance), as it was noted that several technological breakthroughs occurred in the year 2008, e.g.: Google processed 1 trillion URLs [34]; Facebook reached 100 million users [35]; the first Android phone [36]; and Reality Mining [37], a system that uses cell phone data to extract patterns about users. Finally, we selected "peer reviewed" and scientific publications. As a result, we ended up with 78 articles on 'Cyberprivacy' and 564 articles on 'Cyber Privacy', which are the basis of this study.

[1] Finna is a search service that provides central access to material from Finnish libraries and all modern databases and content providers. Finna can be accessed online at: finna.fi

3.2 Scanning, Inclusion and Exclusion Criteria

Articles were assessed afterwards by examining keywords, abstracts, and summaries. Figure 1 shows the process of selecting the relevant articles.

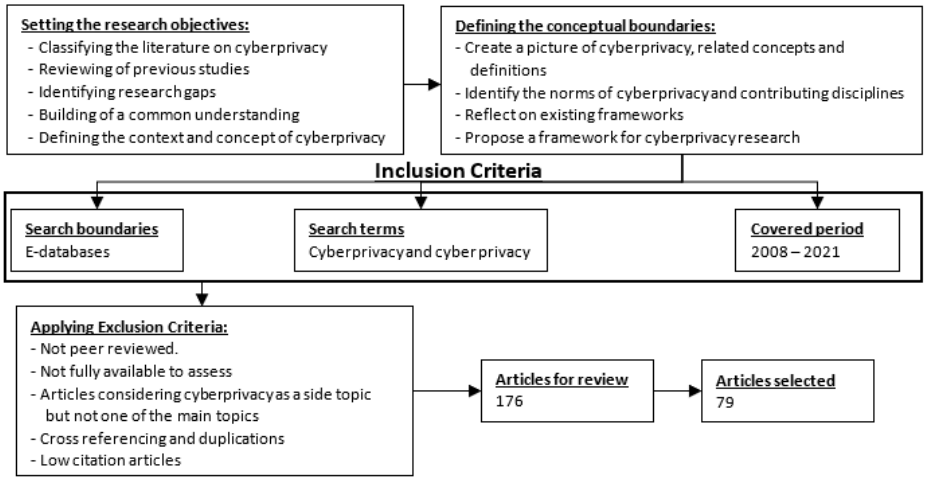

Figure 1: Scanning, inclusion, and exclusion criteria

From selected papers, the following preliminary data was extracted: Number of papers per year (Figure 2a); and Cyberprivacy-related topics and concepts (Figure 2b). The latter was done by counting keyword frequencies. Topics and concepts are then used for our synthesis, which is discussed in Sections 4 and 5.

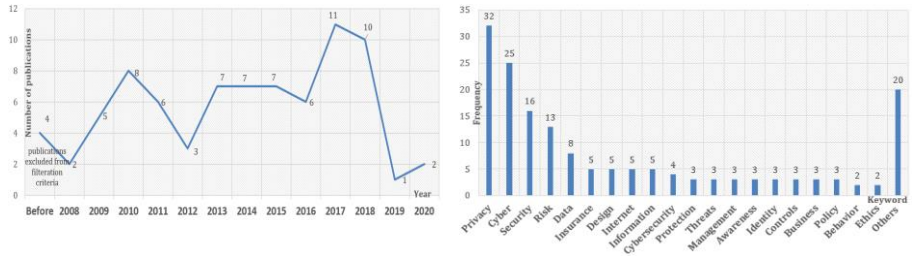

Figure 2: (a) Number of reviewed contents per year; (b) Frequency of keywords extracted from the reviewed literature

4 Findings

4.1 Cyberprivacy Context

Articles were classified into contexts based on the topic and area of concern, so that interpretation and relationship discovery could be conducted. Here we used the qualitative content research methodology practices specified in [38, 39] to help with this task. As a result, eight contexts were found, as shown in Table 1.

Table 1. Common context categories for analysis

Context	Topics and areas of concern
Technology	Applications, developments, and advances in applied knowledge (e.g., technologies and their challenges)
Legislation and rights	Law matters, Acts, constitutions, rights, and regulations
Ethics and morality	Values, beliefs, principles, and the general sense
Business and economy	Profitability and revenue making
Risk and insurance	Threats, danger, assets' loss, impacts and their probability
Behavior and psychology	Perception, acceptance, interpretation, thinking, and actions
Societal	Impact on the society, social matters, and the public
Medical	Health, and well-being

Figure 3 shows the number of articles in each context, noting that an article can fit into more than one context.

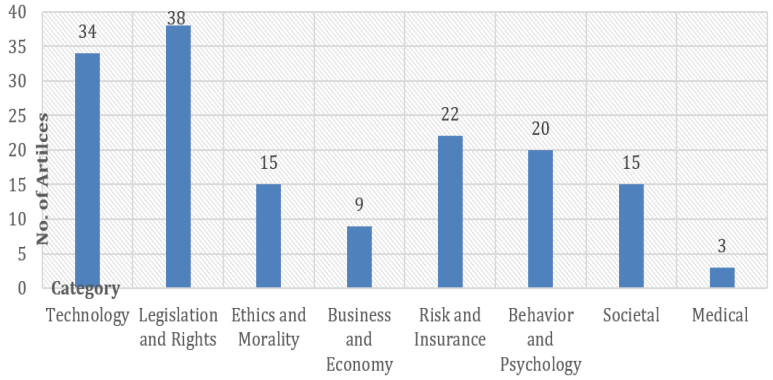

Figure 3: Number of articles concerning cyberprivacy context categories

Cyberprivacy in Technology Context. Services pose privacy risks through the data they collect and process [11], to create clusters and user profiles [11, 40], and in many cases PII [41] can be identified even after implementing some level of data obfuscation. Technologies allow revealing sensitive information, such as identities, physical features, biometric information [42], time, location, and used applications [43, 44]. Cyberprivacy in technology context thus aims to protect the digital persona while taking different forms, i.e. physical, virtual [9], or anonymous [45], since profiling and disclosing information about activities can lead to bigger problems [11, 40]. Table 2 summarizes technologies often discussed in selected papers.

Table 2. Technologies and their challenges for cyberprivacy

Technology	Challenges for cyberprivacy
Cookies [11]	Keep users' data and identifiers that contain personal attributes and thus can be used for tracking

Technology	Challenges for cyberprivacy
RFID and NFC [46, 47]	Allow monitoring and tracking and thus can be used to reveal personal activities
Data science and knowledge discovery [48]	BD, DM, DL, and AI, have great capabilities to learn users' activities and create users' profiles and their behavior [40]
IoT [49, 50]	Monitor, track, and control data, such as in Smart Grid [51, 52, 53], and Smart Cities [54, 55]
VR and AR [9]	Not only track the user, but others around VR/AR

Several papers addressed solutions to deal with those challenges in cyberprivacy [48, 56]. For example, law must address the use of emerging technologies, and similarly new technologies must take the law and regulations at their core. Moreover, solutions such as encryption and anonymity are no longer the key [42, 45, 49, 53, 57], since tracking can be done without decryption. Literature also discussed using technologies as a means to deal with those challenges. For example, blockchain can solve some of the mentioned issues as blockchain underpins encryption, anonymity, and traceability simultaneously, and thus can be used as a trusted third party [57]. Also, advanced encryption (e.g., asymmetric encryption or public key cryptography) should be included from the design [58] phase. Finally, subgroups and protected zones where privacy is measured differently [59], control and opting mechanisms [43, 60, 61], and systems' compatibility [59], should be considered.

Cyberprivacy in Legislation and Rights Context. Cyber governance is considered a complex task to regulations [12]. Many dilemmas and aspects have been discussed in selected papers. For example, the distinction between information that could be public or should be kept private [12]; self-regulation [43]; free speech against knowledge dissemination [62] and security; personal information [11] and useful utilizations [45]; public's safety [63, 64] versus privacy; the rights of liberty [12, 65] and democracy [46, 66, 67]; cyber terrorism and other cyber-backed illicit activities as bullying, stalking, misinformation, etc. [68]; political and governmental rights [1, 69, 70]; law consideration [7] and the way actions in cyberspace are perceived and evaluated; regional and global differences in viewing privacy rights [3, 71].

Cyberprivacy measures therefore are the key to resolving these dilemmas and aspects. Many articles (e.g., [3, 42, 43, 45, 62, 66, 71, 72]) specify that consent and control mechanisms are the key to achieving cyberprivacy. With consent mandated, individuals can accept or deny data collection and/or sharing prior to further processing. Moreover, consent itself requires transparency [1, 7, 59, 62, 64, 66, 73] and sharing of usage information, thus promoting awareness [67, 74, 75]. Control mechanisms play a vital role here as they regulate activities, allowing users to interact, control, and amend data in the event of changes. Acts as the General Data Protection Regulation (GDPR), the Fair Information Practice Principles (FIPPs) [59], and California Consumer Privacy Act (CCPA) [76], addressed this inquiry by mandating data collectors to provide users with safeguards and controls to modify preferences according to their needs. Besides

this, they also mandated the right to seek their own data erasure, which is known as the right to be forgotten [71, 77].

Law enforcement and accountability are a key to protecting cyberprivacy and ensuring systems that operate as expected. However, there is no common agreed legal framework for cyber activities [66]. As a result, awareness of legal consequences and liabilities should be informed and enforced. Moreover, some laws and regulations have shortcomings [45, 78] regarding data disclosure and prohibition of data collection. To overcome these obstacles, an independent legal privacy authority is needed to assess, mediate, and enact rules and policies that address these issues [45, 73, 78, 79, 80].

Cyberprivacy in Ethics and Morality Context. Ethics and morality are considered as one of the important topics in selected papers [68, 81]. For example, literature have discussed about anonymity; sharing information on cyberspace; sharing of personal records [82]; communication ethics; piracy [83] and using copyrighted or outdated materials; demographic data collection transparency; and ethics of new cutting-edge technologies (e.g., VR [9], DM [8], tracking technologies [47], and autonomous vehicles [3]).

Cyberprivacy can be viewed from two perspectives. First, cyberprivacy concerns the morals and ethics of personal rights [8, 84], and thus protects against technological harm and misuse of personal information [68]. Second, too much privacy is against morality [3], as it can be misused for illicit activities or to hide information that can prevent other sorts of harm. To balance these contradictions, cyberprivacy needs to be considered in context rather than in abstract [8], and people can be objectified to understand their needs in concrete rather than in abstract [81]. As a result, the concept of moral mediators was introduced [81] to help understanding the morality of relationships between objects and humans. Furthermore, the concept of privacy and belonging to the persona needs revising [46] since objectifying privacy brings up the concept of ownership [3] and intellectual property rights mentioned earlier. Such application is thus seen beneficial in many ways, since it can resolve many of the contentious issues between technology and the right to privacy, e.g. censorship of individuals and services [67], violations by some governments or service providers [85, 86].

Cyberprivacy in Business and Economy Context. Many businesses rely on data to optimize services and reach consumers [87]; however, their practices may lead to privacy violations, and the spread of misinformation [41] and spam. PII is beneficial to the business; yet, data collection methods have the capacity to address a person more precisely than needed. Accordingly, literature has raised significant concerns, such as incidents [87] as database theft or data tampering [60].

Also, questions about the relationship and importance of cyberprivacy and trust to business have been discussed in literature [48, 87], as well as the need for privacy measures in technology and business for economic growth [85, 86]. For example, it has been shown that in developing economies [88] cyberlaw played a vital role in recovery and building business trust [85, 86]. The same was also seen [48] when well-known

business brands suffered value loss due to opaque practices and lack of privacy safeguards [60]. Other issues that have been discussed in selected papers are open supply chain and information access since they are associated with data ownership rights' risks [48], and practices of businesses asking for more information than required, as in social accounts and credit card approval [41].

Cyberprivacy in Risk and Insurance Context. Cyber risks are mostly intangible [54, 55] and have broad impacts on many levels. For example, cyber risks can lead to the loss of some rights in favor of other interests [9], they also can trigger interference and influence decision-making [89]. From selected papers, cyber risks can be grouped into two categories: risks that affect security and integrity of systems, and risks that affect users and their rights (e.g., privacy, possession, and control). Regarding privacy, the use of data for operations has brought several challenges, such as data ownership rights, lack of a standardized model to develop security and privacy techniques [90], the tradeoff between protection and utility [59], and misleading regulations [9, 48, 91, 92, 93, 94, 95]. As a result, many risks have been discussed, including social networking data manipulation and privacy issues [96]; marketing and service tracking technologies [10]; VR and AR [9]; and risks of lack of awareness [97].

Literature has discussed risk management as a tool to help reduce the impact of these risks by identifying and quantifying privacy risks according to significance and impact, and ensuring compliance with standards and established agreements [59]. Risk management can also help delegate and transform risks into monetary value [98]. However, most cyber risks do not have such an option as policies require physical proof of loss or damage [79, 80]. Still, it is possible to overcome these limitations by framing privacy as an intellectual property [99] and considering cyber risks as operational and technical incidents. Literature also discussed the cautiousness of insurers in offering cyber liability solutions due to the increase in the attack surface [90] and changes in cyberlaw [91, 92, 93, 94, 95]. In fact, less than 10% of insurers cover cyber risks [99].

Cyberprivacy in Behavior and Psychology Context. Literature has discussed in this context, for example, that the identity [84], self-expression, and behavior [7, 67, 84] have changed in cyberspace. This is because of the state of the cyborg [68, 100], interaction on social media [84, 96], and acting differently while wearing different identities [3]. As a result, the meaning of harm itself changed as it shifted more towards emotional and social [7, 84] harm, through discrimination and shame [46].

Cyberprivacy has much to do with these changes, such as being known to many circles [7, 46], being monitored while exercising rights [46], bullying, stalking, intimidation, harassment, and spreading misinformation [68, 96]. This was evidenced in [7, 101, 102, 103] where violence erupted through technology and increased visibility. Moreover, many prefer reasonably priced services with privacy safeguards than free services without any [96, 98]. Accordingly, privacy-centric solutions [46] should be always the first option to consider. Attention should be paid to creating awareness and disseminating information as users tend to be the weakest link [97]. Yet, for effectiveness, awareness should come from a high trustworthy authority [104] to be

accepted and fully adopted by end-users. Finally, psychological mediators [81] should be considered as they help form reasoning about actions and behavior.

Cyberprivacy in Society Context. From a societal perspective, two views are discussed: the right to be left alone and the need for societal interaction [11]. To balance these views, it is necessary to preserve privacy norms while engaging in social and societal activities by taking measures regarding sharing and sensitivity of information, and defining attributes to preserve privacy [59, 88, 105]. Accordingly, it is important to specify private and public attributes, deploy means for controlling own data, and balance the societal benefits of sharing information with privacy needs [59, 106].

One of the solutions is to create different spheres (e.g., private, public) to exercise rights within [66]. Another solution is defining privacy depending on the group-level since the meaning of privacy varies according to the group [64]. Nevertheless, it is necessary to update privacy for the society [78] and review technologies, regulations, and policies, to ensure compliance and consistency with privacy norms.

Cyberprivacy in the Healthcare Sector Context. The healthcare sector [106] has been always driven by personal data, thus [45] has considered ensuring data integrity and availability, as well as an adequate level of privacy. One issue is the significant privacy risks considering current technologies capabilities for identification of individuals. Trust in the healthcare sector is vital, as records can be used for inappropriate purposes. Still, information and data should be available to authorized parties upon request, to provide services and assistance as needed. Recently, health and fitness Apps and services have been a concern as they can pose privacy infringements. Accordingly, this issue requires careful consideration.

4.2 Cyberprivacy Definitions

As discussed previously, different views exist on cyberprivacy. E.g., the technical side views data as belonging to systems, and thus can be used for services and optimization. The legislative side views privacy and information as a protected right of owners. The commercial side sees data as an enabler to provide insights about consumers, etc. In Table 3, we developed and summarized the definitions related to cyberprivacy.

Table 3. Common context categories for analysis

Concept	Definition
1. Cyberprivacy (Technical view)	An extension of the domain of physical privacy in cyberspace, thus following the reasoning of what is permitted and what is not in physical domains
2. Cyberprivacy (Sociotechnical view)	The collective set of norms and measures necessary to protect and control the activities and characteristics of cyber-identity in cyberspace and related domains

Concept	Definition
3. Cyberprivacy (Rights view)	A concept that aims to maintain the rights to privacy, freedom, self-expression, self-determination, and reasonable behavior across cyberspace, and thus it is the intellectual ownership and accountability for storing, processing, and sharing information in cyberspace
4. Cyberprivacy (Legislation view)	A protection layer that aims to raise awareness against misuse of personal data, enforce control, and seek to amend data and attributes of pre-established relationships when needed

4.3 Issues of Cyberprivacy

The issue of cyberprivacy comes from the definition of identity and the prevalence of similar characteristics, the morals and ethics behind processes, and the transformation of humans into cyborg-like entities [3, 7, 8, 81, 84]. Although these are psychological and sociological changes, they only have resulted from advances in the ICT sector [107], as shown in Table 4.

Table 4. Advances in the ICT Sectors

Issue	Advances
Storage	High-density; New architectures; Cloud management; Remote management; & Data resiliency and Recovery protection
Processing and Recognition	Distributed Computing; Cloud; Natural Language Processing; Image and Voice Recognition; & Enabling new technologies: ML, AI, VR, and AI.
Communication	Enabling new technologies: SG, IoT, and SCs; Network and Telecom technologies; Connectively clouds and Quantum networking; Content sharing; real-time streaming; & Social media integration with e-services accounts
Data	BD, DM, Data visualization, and advances in data science; Automated data categorization; Precise analytics, statistics, and forecasting; & Profiling

5 Discussion

Cyberprivacy is a set of concepts and solutions that collectively provide protection against leakage of personal information and data. This makes it clear how cyberprivacy differs from cybersecurity and data privacy as cyberprivacy is a holistic concept that incorporates technical and non-technical issues within. Regarding implementation, the main approach to achieving cyberprivacy is to define core and conceptual protection measures and then proceed with the technical ones, bearing in mind that conceptual and technical measures are required simultaneously. Based on contexts and issues of cyberprivacy, we define the layers required to achieve cyberprivacy as in Figure 4.

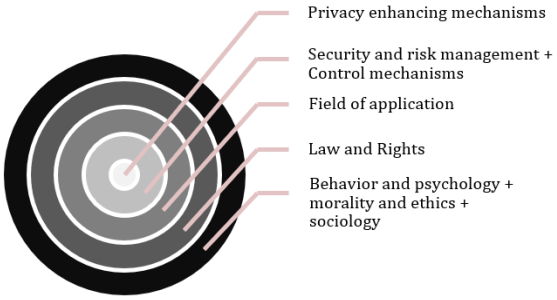

Figure 4: Layers of Cyberprivacy

Cyberprivacy is arranged in five layers that cover needs. First, norms and standards should be defined based on interaction and communication needs, then measured against moral and ethical standards to monitor their behavioral and psychological outcomes, and thus regulate and modify them as required. For this step, general frameworks of ethics and morality must be referred to, in addition to allowing a certain degree of flexibility, to suit different societies. Second, laws and regulations should define rights and obligations, what is permitted and what is not, and ensure enforcement through continuous monitoring of operations and processes. Here, laws and regulations should consider the scope and area of application, and therefore it is recommended to develop and use regulations that can be widely applied, e.g. GDPR. Third, the field of application brings specific and customized rules and policies of the sector or domain concerned, since these rules differ from one field to another.

The fourth- and fifth-layers deal with the application of the criteria, concepts, and approaches defined from the previous conceptual layers. Risk management is considered, thus to assess general risks of norms of the first two layers and specific risks associated with the field of application layer. Based on the results, measures are selected and adjusted. In particular, measures are based on cybersecurity and information security practices; however, control and monitoring mechanisms need to be integrated, to allow different parties to access, control, and monitor data based on permissions, privileges, and sensitivity. Finally, the fifth layer includes mechanisms to enhance and promote privacy; accordingly, this layer must consider anonymity and traceability. Anonymity can protect individuals and maintain the privacy of their data even in the event of data tampering, since data will not be linked to a specific entity. Traceability is required for communication, and to prove accountability for actions and information sharing. To enhance privacy, both criteria should be considered equally, thus permitting privacy without compromising or misusing the right. For this, identities should be separated from communication by means of using pseudonyms, and implementing separate identity domain management systems to provide linking and disengaging functions as required. Still, mechanisms for data removal after processing, opting out, changes tracking, and private data erasure, should be included.

Regarding the practical part, although out of the scope of this study, we have come across several solutions that can be used to provide a certain level of data privacy at the application layers, e.g. obfuscation [2, 53, 55], anonymizers [11, 41, 85], end-to-end

encryption [45, 53, 57], Public Key Infrastructure [46, 53, 57, 60, 66, 77, 85], differential privacy [2, 19, 51, 53, 55, 59, 77], k-anonymity [19, 53, 55, 59, 77, 82, 96, 104, 108], data minimization [40, 53, 59], Blockchain [56, 109], and others. However, as mentioned, these are methods of data privacy, but to achieve the level of protection targeted by cyberprivacy, protection should be considered across all layers simultaneously.

6 Conclusion, Future Research, and Limitations

We have addressed the topic of cyberprivacy in this study in the aim of understanding the context, concept, and cyberprivacy-related issues. We conducted a literature review on cyberprivacy and selected 79 papers for the study. We contribute to literature by providing eight contexts of cyberprivacy and their characteristics, i.e., technology, legislation, ethics, business, risk, psychology, society, and healthcare. These contexts indicate that cyberprivacy is not a single discipline, but it is an interdisciplinary approach that involves drawing appropriately from several disciplines to redefine problems outside of normal boundaries and reach solutions based on a new understanding of complex phenomena. We also contribute by providing the concepts of cyberprivacy in different views, i.e., technical view, sociotechnical view, rights view, and legislation view.

This study opens several opportunities for future research. First, future research should pay more attention to the four issues of cyberprivacy that emerged from this study, that is storage, communication, data, and processing and recognition. We argue that it is crucial to address these issues before they develop further in a negative way. Second, rapid digitalization, and technological change have been disrupting traditional norms in recent years [110, 111]. This indicates the importance of cyberprivacy in the new normal. As a result, an in-depth study on cyberprivacy in different contexts in digital transformation would strengthen our understanding on the subject, and it thus would help protect privacy in cyberspace. Third, there is an increasing ratio of renewable and decentral energy generation around the world [112]. This leads to growing trends in integration of ICT into electrical power systems, such as smart meters in households are connected to IoT devices over the Internet. This trend also brings cyberprivacy and cybersecurity threats to energy systems [113]. A study on cyberprivacy issues on the energy system is thus valuable for different parties as it could help to prevent physical consequences and very costly damages of data breaches in the energy system. Moreover, given that there is limited information regarding the educational perspective of cyberprivacy in selected papers, a study on cyberprivacy in higher education study programs would enhance cyberprivacy awareness and it also would help educate professionals in the field of cyberprivacy.

This study itself has its limitations. First, we focused on three databases: IEEEXplore, Finna, and Google scholar. Although Google scholar can cover all papers, some papers might not yet appear and thus were excluded from the study. Second, the time period of searching is 2008 to June, 2021. Articles accepted and published at the beginning of 2021 may not have been indexed by that point, and were thus excluded.

References

1. Demchak, C. C., and Fenstermacher, K. D. “Institutionalizing Behavior Based Privacy”. Admin. & Society, 41.7, 2009, pp 783-814.
2. Cranor, L. et al. “Towards a privacy research roadmap for the computing community”. arXiv preprint arXiv:1604.03160, 2016.
3. Magnani, L. “Chapter Seven Knowledge as a Duty: the ethical significance of the interest in information and knowledge”. Computing and Philosophy in Asia, 108, 2009.
4. Russell, D. et al. “Computer security basics”. O’Reilly, 1991.
5. Biselli, Tom, and Christian Reuter. "On the relationship between it privacy and security behavior: A survey among german private users." (2021).
6. J. Ma et al., “Perspectives on cyber science and technology for cyberization and cyber-enabled worlds”. Proc. CyberSciTech, New Zealand, 2016, pp 1-9.
7. Magnani, L. “Structural and technology-mediated violence: Profiling and the urgent need of new tutelary technoknowledge”. Intl. J. of Technoethics (IJT), 2.4, 2011, pp 1-19.
8. Magnani, L. “Abducing personal data, destroying privacy: diagnosing profiles through artefactual mediators”. Privacy, Due Process and the Computational Turn, Routledge, 2013, pp 81-104.
9. Yadin, G. “Virtual Reality Surveillance”. Cardozo Arts & Ent. L. J., 35, 2016, pp 707
10. Kimrey, B., and Clark, B. “Cyberprivacy and Digital Privacy Risks”. Comm. L., 29, 2012, pp 10.
11. Berghel, H. “Cyberprivacy in the new millennium”. Comp., 34.1, 2001, pp 132-134.
12. Post, D. “Cyberprivacy, or What I (Still) Don't Get”. Temp. Pol. & Civ. Rts. L. Rev., 20, 2010, pp 249.
13. Warren, S. D., and Brandeis, L. D. “The right to privacy”. Harvard L. Rev., 1890, pp 193-220.
14. Agre, P. E., and Rotenberg, M. “Technology and privacy: The new landscape”. MIT Press, 1998.
15. Loch, K. D., Conger, S., and Oz, E. “Ownership, privacy and monitoring in the workplace: a debate on technology and ethics”. J. of Bus. Ethics, 17.6, 1998, pp 653-663.
16. Foxman, E. R., and Kilcoyne, P. “Information technology, marketing practice, and consumer privacy: Ethical issues”. J. Public Policy & Marketing, 12.1, 1993, pp 106-119.
17. Hitachi Systems Security Inc. “Is Cybersecurity the Same as Data Privacy?” 2019, https://www.hitachi-systems-security.com/blog/is-cybersecurity-the-same-as-data-privacy/
18. Bashir, M. et al. “Information Privacy: Current and future research directions”. iConference, 2016.
19. “National Privacy Research Strategy”. Nat. Sci. Tech Council. 2016
20. Sponsler, C. “Cyberpunk and the Dilemmas of Postmodern Narrative: The Example of William Gibson”. Cont. Lit., 33.4, 1992, pp 625-644.
21. Mohamed, S. “Consensual hallucination & William Gibson”. 2010.
22. Singer, P. W., and Friedman, A. “Cybersecurity: What everyone needs to know”. Oup, USA, 2014.
23. Dukes, C. W. “Committee on national security systems (CNSS) glossary”. CNSSI, Fort Meade, MD, USA, Tech. Rep, 4009, 2015.
24. Craigen, D., Diakun-Thibault, N., and Purse, R. “Defining cybersecurity”. Tech. Innov. Mgmt Rev, 4.10, 2014.
25. “Framework for improving critical infrastructure cybersecurity”. Nat. Inst. Std. Tech. NIST, 2014, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf/

26. Thuraisingham, B. “Data mining, national security, privacy and civil liberties”. ACM SIGKDD Explorations Newsletter, 4.2, 2002, pp 1-5.
27. Taipale, K. A. “Data mining and domestic security: Connecting the dots to make sense of data”. Columbia Sci. Tech. L. Rev., 5.2, 2003.
28. Hayes, B. “Connecting the dots”. American Sci., 94.5, 2006, pp 400-404.
29. Seifert, J. W. “Data mining and the search for security: Challenges for connecting the dots and databases”. Govt. info. Qtly., 21.4,2004, pp 461-480.
30. Okoli, C., and Schabram, K. “A guide to conducting a systematic literature review of information systems research”. 2010.
31. Schryen, G. “Writing qualitative IS literature reviews—guidelines for synthesis, interpretation, and guidance of research”. Comm. Assoc. Info. Sys., 37.1, 2015, pp 12.
32. Rowe, F. “What literature review is not: diversity, boundaries and recommendations”. 2014.
33. Capurro, R., Eldred, M., and Nagel, D. “Digital whoness: identity, privacy and freedom in the cyberworld”. Walter de Gruyter, 2013.
34. Manovich, L. “Cultural analytics: visualising cultural patterns in the era of “more media”. Domus March, 2009.
35. Kelly, K. “The new socialism: Global collectivist society is coming online”. Wired Mag., 17.6., 2009, pp 17-06.
36. Godwin-Jones, R. “Emerging Technologies–Mobile-computing trends: lighter, faster, smarter”. Lang. Lrn. Tech., 12.3, 2008, pp 3-9.
37. Eagle, N., and Pentland, A. S. “Reality mining: sensing complex social systems”. Pers. ubiquitous Comp., 10.4, 2006, pp 255-268.
38. Hsieh, H. F., and Shannon, S. E. “Three approaches to qualitative content analysis”. Qual. H. Res., 15.9, 2005, pp 1277-1288.
39. White, M. D., and Marsh, E. E. “Content analysis: A flexible methodology”. Lib. trends, 55.1, 2006, pp 22-45.
40. Berghel, H. “PII, the FTC, Car Dealers, and You”. Comp., 47.5, 2014, pp 102-106.
41. Levit, N. “Family privacy bibliography”. J. American Acad. Matrimonial Lawyers, 17, 2009, pp183-255.
42. Bellaby, R. W. “Going dark: anonymising technology in cyberspace”. Ethics Info. Tech., 20.3, 2018, pp 189-204.
43. Sessler, J. B. “Computer cookie control: Transaction generated information and privacy regulation on the Internet”. J. L. Plcy., 5, 1996, pp 627.
44. Dodig-Crnkovic, G., and Horniak, V. “Togetherness and respect: ethical concerns of privacy in Global Web Societies”. AI Soc., 20.3, 2006, pp 372-383.
45. Kumar, S. R. et al. “Data-mining a mechanism against cyber threats: A review”. Intl. C. Innov. Cyb. Sec, IEEE, 2016, pp 45-48.
46. Peslak, A. R. “An ethical exploration of privacy and radio frequency identification”. J. Bus. Ethics, 59.4, 2005, pp 327-345.
47. Cooper, T., Faseruk, A., and Johnson, L. D. “Impact of Privacy and Confidentiality on Valuation: An International Perspective”. J. Fin. Mgmt. Anlys., 23.2, 2010.
48. Sadeeq, M. A. et al. “Internet of Things security: a survey”. Intl. C. Adv. Sci. Eng. ICOASE, IEEE, 2018, pp 162-166.
49. Lu, Y., Papagiannidis, S., and Alamanos, E. “Internet of Things: A systematic review of the business literature from the user and organisational perspectives”. Tech. Forecasting Soc. Change, 2018, pp 136, 285-297.
50. Liu, E., and Cheng, P. “Mitigating cyber privacy leakage for distributed dc optimal power flow in smart grid with radial topology”. IEEE Access, 6, 2018, pp 7911-7920.

51. Knapp, E. D., and Samani, R. "Chapter 4 Privacy Concerns with the Smart Grid". Appl. Cyb. Sec. Smart Grid, 2013, pp 2087-99.
52. Fhom, H. S., and Bayarou, K. M. "Towards a holistic privacy engineering approach for smart grid systems". Intl. C. Trust Sec. Priv. Comp. Comm., IEEE, 2011, pp 234-241.
53. Elmaghraby, A. S., and Losavio, M. M. "Cyber security challenges in Smart Cities: Safety, security and privacy". J. Adv. Res., 5.4, 2014, pp 491-497.
54. Braun, T. et al. "Security and privacy challenges in smart cities". Sustain. Cities Soc., 39, 2018, pp. 499-507.
55. Froomkin, A. M. "The death of privacy". Stan. L. Rev., 52, 1999, pp 1461.
56. Monti, M. et al. "An alternative information plan (Working paper)". Santa Fe Institute, 2017.
57. Adee, S. "Internet architecture". New Sci., 228.3051, 2015, pp 38-39.
58. Thuraisingham, B. et al. "Towards a Framework for Developing Cyber Privacy Metrics: A Vision Paper". Intl. Congress Big Data, IEEE, 2017, pp 256-265.
59. Palmer, C. C. "Preface: cybersecurity for a smarter planet". IBM J. Res. Dev., 58.1, 2014, pp 0–1.
60. Sovern, J. "Opting in, opting out, or no options at all: The fight for control of personal information". Wash. L. Rev., 74, 1999, pp 1033.
61. Bautista, A. "2010 Annual Survey: Recent Developments in Sports Law". Marq. Sports L. Rev., 21, 2010, pp 667.
62. Hansen, L., and Nissenbaum, H. "Digital disaster, cyber security, and the Copenhagen School". Intl. studies Qtly., 53.4, 2009, pp 1155-1175.
63. Simpson, B., and Murphy, M. "Cyber privacy or cyber surveillance? Legal responses to fear in cyberspace". 2014
64. Etzioni, A., and Rice, C. J. "Privacy in a cyber age: Policy and practice". Springer, 2015.
65. Schwartz, P. M. "Privacy and Democracy in Cyberspace." 2017.
66. Jin, C. H. "Self-concepts in cyber censorship awareness and privacy risk perceptions: What do cyber asylum-seekers have?" Comp. Hmn. Behav., 80, 2018, pp 379-389.
67. Isfandyari-Moghaddam, A. "Rocci Luppicini: Ethical impact of technological advancements and applications in society". 2013.
68. Bartholomew, M. "Intellectual Property's Lessons for Information Privacy". Neb. L. Rev., 92, 2013, pp 746.
69. Chatterjee, D. K. "Encyclopedia of Global Justice: A-I". Springer Sci. Bus. Media, 2011.
70. Saxby, S. "The 2012 CLSR-LSPI seminar on privacy, data protection & cyber-security". Intl. C. Lgl. Sec. Priv. Issues IT L. LSPI. Comp. L. Sec. Rev., 29.1, Athens, 2013, pp 4-12.
71. Black Jr, J. E. "Privacy Liability and Insurance Developments in 2012". J. Inet. L. 16, 2013, pp 3-12.
72. Reddick, C. G. "Citizens and e-government: Evaluating policy and management". Info. Sci. Ref., 2010.
73. Nolan, D. R. "Privacy and profitability in the technological workplace". Info. Tech. World Work, Routledge, 2017, pp 203-227.
74. Levinson, A. R. "Toward a cohesive interpretation of the electronic communications privacy act for the electronic monitoring of employees". W. Va. L. Rev., 114, 2011, pp 461.
75. Yu, S. "Big privacy: Challenges and opportunities of privacy study in the age of big data". IEEE access, 4, 2016, pp 2751-2763.
76. Huddleston, J. "Preserving Permissionless Innovation in Federal Data Privacy Policy". J. Inet. L., 22, 2019, pp.17-18.
77. Rosenzweig, P. "Cyber warfare: how conflicts in cyberspace are challenging America and changing the world". ABC-CLIO, 2013.

78. Breaux, R. W., Black, E. W., and Newman, T. “A Guide to Data Protection and Breach Response-Part 1”. Intellect. Property Tech. L. J., 26.7, 2014, pp 3.
79. Breaux, R. W., Black, E. W., and Newman, T. “A guide to data protection and breach response-part 2”. Intellect. Property Tech. L. J. 26.8, 2014, pp 23.
80. Magnani, L. “Material Cultures and Moral Mediators in Human Hybridization”. Intl. J. Technoethics IJT, 1.1, 2010, pp 1-19.
81. Hildebrandt, M. “Profile transparency by design? Re-enabling double contingency. Privacy, due process and the computational turn: The philosophy of law meets the philosophy of technology”. 2013, pp 221-46.
82. De George, R. T. “The ethics of information technology and business”. John Wiley & Sons, 2008.
83. Wiafe, I., Yaokumah, W. and Kissi, F.A. “Students' Intentions on Cyber Ethics Issues”. Mod. Theor. Prac. Cyber Ethics Sec. Compl, IGI Global, 2020, pp 105-121.
84. Warwick, K. “Cyborg morals, cyborg values, cyborg ethics”. Ethics Info. Tech., 5.3, 2003, pp 131-137.
85. Cross, F. B., and Miller, R. L. “The Legal Environment of Business: Text and Cases: Ethical, Regulatory, Global, and Corporate Issues”. Cengage Learning, 2011.
86. Quaddus, M., and Achjari, D. “A model for electronic commerce success”. Telecom. Plcy., 29.2-3, 2005, pp 127-152.
87. Karake-Shalhoub, Z., and Al Qasimi, L. “Cyber law and cyber security in developing and emerging economies”. Edward Elgar Publishing, 2010.
88. Thiele, R. D. “The new colour of war–Hybrid warfare and partnerships”. World Politics Sec., Rio de Janeiro: Konrad Adenauer Foundation, 2015, pp 47-59.
89. Barrett-Maitland, N., Barclay, C., and Osei-Bryson, K. M. “Security in social networking services: a value-focused thinking exploration in understanding users’ privacy and security concerns”. Info. Tech. Dev., 22.3, 2016, pp 464-486.
90. Biener, C., Eling, M., and Wirfs, J. H. “Insurability of cyber risk: An empirical analysis”. Geneva Papers Risk Ins. Issues Practice, 40.1, 2015, pp 131-158.
91. Eling, M., and Schnell, W. “What do we know about cyber risk and cyber risk insurance?” J. Risk Fin., 2016, pp 474-491.
92. Marotta, A. et al. “Cyber-insurance survey”. Comp. Sci. Rev., 24, 2017, pp 35-61.
93. Romanosky, S. et al. “Content analysis of cyber insurance policies: How do carriers write policies and price cyber risk?”. 2017.
94. Woods, D. et al. “Mapping the coverage of security controls in cyber insurance proposal forms”. J. Inet. Servs. Apps., 8.1, 2017, pp 8.
95. Thakur, K., and Kumar, H. “Challenges in protecting personated information in cyber space”. Intl. C. Emerging. Trends Nets. Comp. Comms. ETNCC, IEEE, 2015, pp 167-171.
96. Yan, Z. et al. “Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment?”. Comp. Hmn. Behav., 84, 2018, pp 375-382.
97. Bughin, J. “Digital user segmentation and privacy concerns”. J. Direct Data Dig. Mktg. Practice, 13.2, 2011, pp 156-165.
98. Wright, M. F. “Cyber aggression within adolescents’ romantic relationships: Linkages to parental and partner attachment”. J. Youth Adolescence, 44.1, 2015, pp 37-47.
99. Murray, A. “Looking back at the law of the horse: Why cyberlaw and the rule of law are important”. SCRIPTed, 10, 2013, pp 310.
100. Magnani, L. “Distributed Morality in a Technological World, Knowledge as Duty”. Keynote speaker: 18, 2007.
101. Wright, M. F. “Intimate partner aggression and adult attachment insecurity: The mediation of jealousy and anger”. Evol. Behav. Sci., 11.2, 2017, pp 187.

102. Crane, C. A. et al. “Problematic alcohol use as a risk factor for cyber aggression within romantic relationships”. Amer. J. Add., 27.5, 2018, pp 400-406.
103. Carpenter, S. et al. “Expert sources in warnings may reduce the extent of identity disclosure in cyber contexts”. Intl. J. Hmn. Comp. Interact., 33.3, 2017, pp 215-228.
104. Lynch, K. “The global drivers of change”. OPTIONS POLITIQUES 2010, 2009.
105. Tschider, C. A. “Enhancing cybersecurity for the digital health marketplace”. Annals H. L., 26, 2017, p 1.
106. “Information and Communication Technologies: A World Bank Group Strategy”. World Bank Pub., 2002
107. Do, C. T. et al. “Game theory for cyber security and privacy”. ACM Comp. Surv. CSUR, 50.2, 2017, pp 1-37.
108. Awan, J. H. et al. “Cyber Threats/Attacks and a Defensive Model to Mitigate Cyber Activities”. Mehran Uni. Res J. Eng. Tech., 37.2, 2018, pp 359-366.
109. Xu, Hao, et al. “BeepTrace: blockchain-enabled privacy-preserving contact tracing for COVID-19 pandemic and beyond”. IEEE Inet. Things J., 2020.
110. Dang, D., and Vartiainen, T. “Digital strategy patterns in information systems research”, PACIS 2019 Proceedings, (2019).
111. Dang, D., and Vartiainen, T. “Changing patterns in the process of digital transformation initiative in established firms: the case of an energy sector company”, PACIS 2020 Proceedings, (2020).
112. Varela, I.: Energy Is Essential, but Utilities? Digitalization: What Does It Mean for the Energy Sector? In: Linnhoff-Popien, C., Schneider, R., and Zaddach, M. (eds.) Digital Marketplaces Unleashed. pp. 829–838. Springer, Berlin, Heidelberg (2018)
113. Dang, D., Vartiainen, T., and Mekkanen, M., “Towards Establishing Principles for Designing Cybersecurity Simulations of Cyber-Physical Artefacts in Real-Time Simulation,” Intl. C. Info. Sys. Dev. (ISD), (2021).