Journal of Business Ethics
https://doi.org/10.1007/s10551-021-04747-x

ORIGINAL PAPER

Could You Ever Forget Me? Why People Want to be Forgotten Online

Chanhee Kwak[1] · Junyeong Lee[2] · Heeseok Lee[3]

Received: 17 September 2019 / Accepted: 13 January 2021

Abstract
The concept of people's memory maintains the finiteness of time and capacity. However, with the advancement in technology, the amount of storage memory a person can use has increased dramatically. Given that digital traces can hardly be erased or forgotten, individuals have begun to express their desire to be forgotten in the digital world, and governments and academia are considering methods to fulfill such wishes. Capturing the difficulties in terms of a cultural lag between technological advancements and regulations on individuals' data privacy needs, we identify six motives for individuals wishing to be forgotten online and investigate its expected effects on online content generation through a qualitative content analysis of 222 responses from open-ended surveys in Korea. Our findings provide implications for the literature on individual privacy and the right to be forgotten employing the cultural lag, as well as, elaborate further on the relationship between being forgotten online and the legitimacy of such requests of individuals. Additionally, implications for data providers, data controllers/processors, and governments to address this lag and build a balanced system of personal information are provided.

Keywords Cultural lag · Right to be forgotten · Individual privacy

Introduction

The general capacity of human memory has dramatically increased with the help of information and communication technologies. People hardly forget the moments of their lives that are recorded and stored digitally, thereby shifting the perception of memory from being volatile to durable. However, as remembering has become the new standard, it has created opposite needs for memory, namely, to be forgotten (Mayer-Schönberger 2011). Large collections of an individual's data encompassing communications, shopping, media consumption, and social networks can unravel a mysterious being into rows of personal data (Richards and King 2013). Individuals have begun to develop a desire for forgetting or being forgotten, as much as for memorizing, because of the potential privacy infringement caused by unforgotten personal data (Cukier and Mayer-Schoenberger 2013).

For an individual, personal data is not always easy to manage (Burkell 2016). Searching one's name on Google exemplifies the difficulties of altering one's personal data online. In a mash-up form of data, medical inquiries, the aggregated usage of social network services, and other delicate information can be easily found on Google, regardless of an individual's consent (Nunan and Di Domenico 2017). However, individuals may not be able to delete disclosed personal data because of technological and legal obstacles. Instead, individuals can request Google to remove links to specific personal data, including the originals, after which Google decides to delete the link. The deletion of photos on Facebook is another example. Although an individual may not want to reveal a certain picture, the individual's friends can upload group pictures that include the individual, without seeking permission. If the individual then tries to delete such photos uploaded by others, Facebook does not delete

✉ Junyeong Lee
junyeong_lee@koreatech.ac.kr

Chanhee Kwak
chk@kangnam.ac.kr

Heeseok Lee
hsl@kaist.ac.kr

[1] Department of Industrial Data Science, Kangnam University, 40 Gangnam-ro, Giheung-gu, Yongin-si, Gyeonggi-do 16979, Republic of Korea

[2] School of Industrial Management, Korea University of Technology and Education, 1600 Chungjeol-ro, Byeongcheon-myeon, Dongnam-gu, Cheonan-si, Chungcheongnam-do 31253, Republic of Korea

[3] College of Business, Korea Advanced Institute of Science and Technology, 85 Hoegiro Dongdaemoongu, Seoul 02455, Republic of Korea

Published online: 01 February 2021

them directly; instead, it suggests sending a message to the uploader to request deletion. Thus, individuals can make deletion requests in both cases but are not guaranteed that those requests will be honored.

The aforementioned examples are closely related to the cultural lag—the gap between technological advances and regulations—that occurs when material culture, which includes physical equipment and its usage, changes faster than nonmaterial cultures, such as ethics, value systems, and laws (Marshall 1999). Although the speed of technological development has accelerated exponentially, the pace of development of laws and regulations has remained virtually unchanged. Therefore, this widening gap between technology and ethics can create new ethical and social problems. If the rules and regulations can be changed quickly enough to catch up with technological development, then digital piracy, cyberbullying, and cyberstalking might be prevented or at least reduced.

To address the cultural lag and mitigate its side effects on individual privacy, existing systems must be revised and new solutions that are rooted in social consensus must be created (Brose 2004). Consensus plays a key role in policymaking and gathering the voices of various stakeholders in a public forum (van de Kerkhof 2006). Guidelines and regulations for technology adoption and its application have been framed by assimilating opinions and finding alternatives (Rachovitsa 2016). Additionally, consensus making can balance interests between society and individuals. Although one may argue that individual rights are supreme to any other legal acts (Gewirth 1978), it is possible to find appropriate and executable solutions between society and individuals by clarifying social consensus. Furthermore, intangible social and cultural values, including ethics and legal rights, can only be considered when social consensus is achieved (Marshall 1999). Such consensus may not be the perfect solution for the society in terms of ethics and righteousness. However, it is important to note that procedural lawfulness is a dependable principle to make agreements in a democratic society.

Thus, the right to be forgotten, a recent solution to reduce the cultural lag regarding individual privacy, should also be based on social consensus. This right's primary purpose is to provide a legal foundation for individuals to manage their personal data when such data manipulations do not harm public interests (European Parliament 2016). Social consensus can resolve the cultural gap that has emerged from the difference between the speeds of technology and regulation in the context of individual privacy. Accordingly, scholars have investigated cross-border and cross-business arbitration proposals to enhance privacy rights in terms of legal clarity, empirical applicability, and the balance between multiple rights (Shahin 2016; Malgieri and Custers 2018). Unfortunately, there is little understanding of why people want to be forgotten, which must be the basis of this right's design and implementation (De Hert et al. 2018). It is hard to determine whether existing forms of implementation of the right to be forgotten reflect the voices of information providers because these forms are usually developed by information controllers (Chenou and Radu 2019). Explorations into determining the need and the right to be forgotten online are necessary to form specifications of this right. Furthermore, understanding such needs are important for balancing the interests of various stakeholders of personal data (Tavani 1999). Therefore, in this study, we aim to answer the following research questions: (1) Why do people want to be forgotten online? (2) What are the expected consequences of the right to be forgotten online?

This study includes a qualitative content analysis of open-ended surveys of Korean Internet users to investigate individuals' motives for wanting to be forgotten in an online context, based on experience, as well as the difficulties of managing private digital records. As a leader in information and communication technologies, Korea has discussed the formulation of privacy rights to restrict access to personal data by third parties and has experienced various privacy issues resulting in strong privacy regulations. Korea has a mature and vibrant Internet culture; thus, it presents a unique testbed for technologies and their effects on people and society. Research findings from the country can benefit not only Korea but also other countries. Our analysis identifies six motives for wishing to be forgotten: information disclosure, content sensitivity, social reputation, control over further processing, system/process, and sociality. Moreover, the survey covers the expected impacts of wanting to be forgotten online and its analysis illustrates how data providers perceive the pros and cons of suitable applications of this right. The findings have implications for the literature on individual privacy and the right to be forgotten with the cultural lag, and can elaborate further on the relationship between being forgotten online and the legitimacy of such requests of individuals. Additionally, our findings provide insights into the individuals, data controllers/processors, and governments to build a balanced system of personal information..

Background

Ogburn (1957) coined the term "cultural lag," which refers to the gap between material and nonmaterial forms of culture. Ethics, traditions, and social norms are parts of nonmaterial culture, whereas technology and equipment are parts of material culture (Roberts and Wasieleski 2012). Although either culture can advance faster than the other, material culture frequently accumulates and progresses much more swiftly because of its exponential speed of evolution, unlike nonmaterial culture, the pace of which has remained virtually constant (Brinkman and Brinkman 1997). For instance,

when a novel technology is introduced to society, material culture advances whereas nonmaterial culture stays put, thereby generating a cultural lag, whose benefits and drawbacks can be determined only after the dissemination of the technology. The rules and regulations can then be proposed as social adjustments to minimize the cultural lag in accordance with social consensus. Different parts of a society are disjointed because of the cultural lag and adjustments among them are required for social stability.

We adopt the theory of cultural lag to investigate individual privacy in modern society. When individuals present their opinions, preferences, and thoughts online, their control over this content seems certain at first—that is, the data is co-controlled by an individual both as the data provider as well as the data controller/processor. However, this is not the case for copied, retweeted, shared, or modified versions of the originals, as the original data provider no longer has control over the new data. When the control of the original data provider is uncertain, any guarantee of individual privacy is meaningless, although it is often observed (Gurevich et al. 2016). At this point, the cultural lag of individual privacy can be observed; societies and nonmaterial culture are unable to keep pace with the rapid changes in technologies and material culture. Consequently, society must make social adjustments to address this lag.

What social adjustments, then, can be made to enhance individual privacy? Introduced by the European Union (EU), the right to be forgotten is one such example. In Article 17, the General Data Protection Regulation (GDPR) defines the right to be forgotten as the right "to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay (European Parliament 2016, p. 43)." We use this as the definition of the right to be forgotten throughout this study. The right originates from a dispute whether an individual can delete online content containing personal information. On the one hand, individuals seem to be eligible to decide the existence of their digital history because their interests are generally the greatest compared to others. Privacy advocates enthusiastically supported the right as it could enhance information autonomy (Newman 2015). On the other hand, the opposition has argued that providing full data control to individuals can result in degraded freedom of expression (Rosen 2011). The main concern was that truthful media reports might be taken down by the right. Furthermore, the overwhelming creation of thoughtless content was also pointed out as a negative consequence of the right. Some argued that the right is too idealistic to be realized (Garcia-Murillo and MacInnes 2018). Following a series of discussions, EU's right to be forgotten states several conditions of enforcements. The right should be applied with respect to the (a) original purpose of data collection and process, (b) withdrawal of the data subject's consent, (c) objection of data collection of the data subject, (d) lawfulness of collection, and (e) legal obligations in the jurisdiction of the data subject.

The bold decision of the EU has changed the rules of the game in the personal data ecosystem. Especially, the GDPR in general and the right in particular shifted more responsibilities on data processors/controllers. Following the guidelines of the right, data processors/controllers need to prepare their criteria and procedures to conform to the EU's regulation, otherwise, they cannot continue their business on the continent. As search engines were directly related to the right, they became the first movers to operationalize it. Google, the biggest search engine operator, established an advisory council to frame criteria for executable guidelines of the right (Tavani 2018). The current process of Google's compliance is based on four criteria: the validity of a delink request, the identity of a requester, the web address, and the source of the information (Bertram et al. 2019). After manual screening by reviewers, the company decides whether to delist links requested by an individual. However, this is a heavy burden for companies operating overseas because they have to tweak details to abide by the rules of the right in each nation, which are not firmly structured in most cases. Although their processes for delisting links regarding personal information are presented, the opaqueness of their decision-making and evaluations seems to be an ambiguous implementation of the right (Chenou and Radu 2019).

Difficulties of search engines have been attributed to the implementation forms of the right not being specified. The EU provides each member country the authority to design implementations to comply with the right. Article 17(3) of the GDPR states when the right might not be applied and includes the conditions when (a) freedom of expression and information is exercised, (b) legal obligations are in effect, (c) public interest of not applying the right is greater, (d) the data is used for research purpose, and (e) legal claims exist (European Parliament 2016). These conditions constitute the GDPR's response to the question of how to balance between the right to be forgotten and other interests. Meanwhile, it opens room for each nation to customize details for implementing the right as it is "a comprehensive privacy framework that must be implemented locally and enforced globally" (Newman 2015, p. 507). It seems a fair decision because the needs of one person can differ from another. As the body of regulation, member countries of the EU have put their efforts into aligning their legal values with the right. Nonetheless, many have difficulties in ensuring effective implementations of the right because of the lack of firm guidelines for the right to be forgotten. For instance, Commission Nationale Informatique et Libertés (CNIL), the French data protection authority, has questioned whether GDPR's guidelines for the right to be forgotten

can be accorded with the French law and its value (Padova 2019). Specifically, according to the original guidelines of the EU, information processors are required to delist links containing personal information from the search results of certain domain names. However, CNIL demanded that the rule of delisting should be applied regardless of a domain name because the same link can be easily found using other domain names of search engine (CNIL 2015). In addition to the territorial scope, ambiguity in creating a balance between multiple interests against the right to be forgotten has been criticized. The French organization pointed out the inconsistency in balancing rules by data protection authorities and the courts.

Discussions regarding the implementation of different forms of the right have spread beyond the EU. Partially inspired by the EU's right to be forgotten, Korea and Japan have actively investigated the alignment of existing legal regulations and the right (Korea Communications Commission 2016; Bobadilla and Atala 2018). Nonetheless, their main concerns do not differ much from that of France and the realization of the right is rather uncertain (Neville 2017). In sum, as the right's implementation goes through a period of transition, the vague guidelines have confused both nations and organizations and effective implementations of the right have a long way to go (Padova 2019; Voss and Castets-Renard 2015).

We argue that the missing link of implementing the right to be forgotten can be closely connected to the understanding of people and social context. Although national boundaries are increasingly becoming fluid in the era of the Internet, it is vital to recognize that people interacted within certain social contexts. This is particularly important for the right as privacy norms are formed based on individuals in social communities (Martin 2016; Rustad and Kulevska 2014), that is, people from different social contexts can interpret the right very differently, and when participants of social communities make privacy-related decisions, their beliefs and behaviors can be significantly affected by various social components including geological (Dinev et al. 2006; Rustad and Kulevska 2014; Shahin 2016), demographical (Lowry et al. 2011), and individual factors such as information change (Lally 1996) and privacy-related experience (Cho et al. 2009). Therefore, to design an implementation model of the right to be forgotten, we need to narrow down to society and its people.

It is worth remembering that the formation of social consensus plays an important role in resolving cultural lag (Marshall 1999; Roberts and Wasieleski 2012). Diverse stakeholders in society have different needs, even when they share the same or identical cultural contexts, leading to unique value systems. By comparing alternatives, sharing opinions, and balancing diverse interests, consensus making entails not only gathering potential needs but also balancing multiple interests by explicitly materializing them (Martin 2016). When it comes to policymaking, consensus making has been the main activity as various stakeholders can share their voices in a public forum (van de Kerkhof 2006). Guidelines and regulations for technology adoption and application have been framed by gathering opinions and finding alternatives (Rachovitsa 2016). Accordingly, if a society can determine a social consensus for a specific cultural lag, the society can proceed with constructive discussions and legislative actions to reduce the lag.

Therefore, understanding the privacy needs of individuals and the right to be forgotten can form an essential part of social consensus from the viewpoint of individuals and act as a starting point for the reduction of the cultural lag (Weber 2010). Hence, in this study, we attempt to expand the research on the right to be forgotten and provide implications of the right's appropriate implementation by answering the following research questions: *Why do people want to be forgotten online? What are the expected consequences of the right to be forgotten online?*

Methods and Data Description

Sample and Data Collection

Issues regarding interpretation and implementation of the right to be forgotten are not limited to a specific region. Although the right originates from the European continent, diverse countries have recognized similar privacy concerns and tried to solve them with legal solutions. For instance, the legislative body of Korea has continuously enhanced privacy regulations to provide similar meaning to the right as intended in the GDPR. Though explicit legislation of the right to be forgotten does not exist, guidelines on the Right to Request Access Restriction on Personal Internet Postings provide individuals with legal rights to seek deletion of personal content regardless of the membership status of the service provider (Korea Communications Commission 2016). The related guidelines focus on the deletion of digital content, which is different from the EU's delink. Thus, Korea is a useful research context for the understanding of technologies and their effects on people and society. Moreover, the research findings from the country can benefit not only Korea but also other countries. To contribute to the formation of the right in the country and even worldwide, we focus on Korea to answer the research questions posed earlier in the study.

To investigate the reasons why people want to be forgotten online and the expected consequences of such a right, we conducted open-ended surveys with a convenience sample. The purpose of open-ended surveys is to explore experiences and gather fresh information about a topic (Sproull 2002).

Compared to the focus group and individual interview methods, greater respondent anonymity can be provided through open-ended surveys (Erickson and Kaplan 2000). It is difficult to measure individuals' motives for wanting to be forgotten and the expected consequences of the right to be forgotten because people acknowledge the necessity of the right to be forgotten only after events impact their personal data. To address this issue, we consider the revision or deletion of personal data as a proxy for wanting to be forgotten. The survey comprised three parts: (1) the (perceived) revision or deletion of online content whose uploader was the subject ("Have you ever revised or deleted 'the content you uploaded online (posts, photos, videos, comments, etc.)'?"), (2) the (perceived) revision or deletion of data when the uploader was only related to the subject ("Have you ever requested to revise or delete 'the online content that you did not upload but was related to you (posts, photos, videos, comments, etc.)'?"), and (3) the perception of the right to be forgotten and respondents' opinions ("What changes do you see in your online content uploads if the right to be forgotten is applied?"). For the first two questions, respondents recalled the experience or their perceptions and then answered the questionnaire. For the third question, we provided the definition of the right to be forgotten and the current situation of the nation's legal preparation, and then, the subjects responded to the questionnaire. The questionnaire was provided in Korean and participation was voluntary with explicit consent. The respondents were allowed enough time to express their thoughts in detail. All questionnaires and instructions in the survey are described in the Appendix in Table 3.

Convenience sampling was used because of its relevance to the research topic rather than the representativeness of how the respondents are selected (Flick 2009). Given that our research topic concerns each individual's need to be forgotten in a general online environment, our sample should consist of individuals familiar with online services and experienced in uploading content on the Internet. Therefore, we collected half of the data from social networking service platforms and the other half by investigating the perceptions of part- and full-time MBA students, government employees, office workers, and students to consider a wider range of ages and occupations. For the first half, we uploaded the post collecting responses mainly on the timeline and group page on Facebook, and additionally, on Twitter and online communities. For the rest, we requested part- and full-time MBA students to participate in the survey during our lecture, and transferred the request to our acquaintance for completing the insufficient samples via KakaoTalk, a dominant instant messenger in Korea similar to WhatsApp.

We collected open-ended surveys from 222 individuals, with meaningful saturation levels (Strauss and Corbin 1990). The survey respondents' demographics are presented in Table 1. Most respondents (203 individuals, or 91.4%) had edited or deleted online content that they had uploaded themselves, while some (73 individuals, or 32.8%) had requested the correction or deletion of online content uploaded by others. Regarding the third question, 137 respondents had knowledge of the right to be forgotten; however, most agreed with the need for the right to be forgotten (208 persons chose "agree" or "strongly agree") when additional information on the definition of the right and related disputes were provided. While 149 respondents wanted a complete deletion (67.1%), 63 preferred delinking (or deindexing, 28.4%), and 10 provided other responses (4.5%).

Data Analysis

Qualitative content analysis was conducted to analyze the data (Ardichvili et al. 2003; Elo and Kyngäs 2008), as our research questions focus on extracting and identifying categories from data (Cho and Lee 2014). The data analysis process had three phases: preparation, organization, and reporting (Elo and Kyngäs 2008). As the preparation phase included selecting the unit of analysis and discerning the data as a whole (Tesch 2013), we read the data carefully to understand the overall content and selected the unit of analysis by identifying, extracting, and synthesizing the text of each question.

The organization phase comprised three steps: open coding, creating categories, and abstraction (Elo and Kyngäs 2008). First, we used an open coding approach to extract codes from the open-ended survey answers (Merriam 2002). During this step, we read the open-ended survey answers thoroughly and iteratively to identify the patterns by reviewing the words or phrases used in the responses, and freely generated codes and categories (Burnard 1991; Elo and

Table 1 Survey participant demographics

Item / Case (Ratio)	
Gender	
Male	115 (51.8%)
Female	107 (48.2%)
Age	
20 s	73 (32.9%)
30 s	110 (49.5%)
40 s	29 (13.1%)
50 s	10 (4.5%)
Occupation	
Employed	156 (70.3%)
Student	49 (22.1%)
Homemaker	5 (2.3%)
Others	12 (5.4%)
Total	222

Kyngäs 2008). The coders content-analyzed not only those segments of the answers to a specific question (for example, "Why did you revise/delete the content you uploaded online?") but also the answers to related questions (e.g., "Was the revision/deletion smoothly practicable?" or "If it was difficult to revise/delete the content you uploaded online, what was the reason?") to find relevant patterns. Following Ardichvili et al. (2003), the coding employed in this study was conducted independently by two researchers.

The list of categories derived from coding was then grouped to arrive at a higher-order heading depending on their interrelationships (Hsieh and Shannon 2005; Elo and Kyngäs 2008). During this step, the number of categories was reduced by collapsing and condensing into broader categories to describe the phenomenon and enhance the understanding of the phenomenon based on interpretation and discussion. The differences between the coders were discussed by three researchers to proceed with the categorization. These discussions involved interpretation and re-contextualization of data and re-analysis and synthesis of relevant segments and categories. The categorization was iteratively updated until all the researchers reached an agreement (Elo and Kyngäs 2008; Ardichvili et al. 2003; Winslow 2003). The open-coded categories in the initial phase were then aggregated through iterative discussions into broader categories of why people revise/delete the content they upload.

In the final step of the creating categories phase, namely, abstraction, we formulated a general description regarding the research topic through categorization with discussions, naming each category with content-characteristics words, and integration (Dey 2003; Elo and Kyngäs 2008). For reporting the process of analysis and the results as research outcomes, we used actual quotes and figures describing an abstraction process for each question (Cho and Lee 2014; Winslow 2003).

Motives and Interpretations

Based on qualitative content analysis of the open-ended survey responses on the reasons people want to delete not only their personal data but also the data of others relevant to their privacy, we identified six categories of motives for wanting to be forgotten: *information disclosure, content sensitivity, social reputation, control over further processing, system/process,* and *sociality.*

Information disclosure The increasing exposure of personal data is one of the main concerns of the respondents. In terms of data disclosure scopes and boundaries, the respondents consider private online content as a source of potential risk because they cannot rule out its possible misuse. The respondents expressed concerns that unauthorized people might utilize or publicize their private content. Some information technology (IT) services, such as Facebook, have recognized this concern and now offer features that allow users to decide who can view each post, such as friends, friends of friends, and the public. However, it is difficult for individuals to manage their personal information in each service. Moreover, even with such options, the possibility of personal data disclosure remains a large risk for individuals who want to protect their privacy and be forgotten. Responses that indicate such concerns include "I do not want my information to be made public" and "I want to prevent people who are not related to me [e.g., strangers] from seeing my content."

Content sensitivity Respondents' concerns can increase when the data contain potentially sensitive information, where *potentially sensitive* means the individuals might not understand the inherent risks of initially uploading the data because of the difficulty in estimating the potential damage due to an increase in accessibility to private content. Through later evaluations of content containing sensitive information, individuals can update their initial risk assessments, which can lead to adjusting the content. Respondents expressed apprehensions, for example, that "the facts on [sensitive] content are wrong" and "the content includes private information." These concerns arise mostly from individuals' evaluation of their content.

Social reputation In addition to individuals' evaluation of their online content, respondents' intentions to modify content were frequently observed to be due to the risk of harming their online or offline reputation, whether or not they had uploaded the content themselves. For example, "It is embarrassing to me" and "It contains content that is harmful to me." Some respondents even deleted all the photos of their school days to mitigate such concerns. Although this motive shares similarities with content sensitivity, the difference lies in the former mainly focusing on individuals' evaluation of their own online content and the latter centering on the public evaluation of the content.

Control over further processing The respondents also considered their content to be potentially at risk because of loss of data control from further processing and the speed of information diffusion. The scope of information use and control appear to be significant concerns for data providers. When data subjects are unclear about the boundaries of the data usage by data controllers/processors or when personal information usage is not clearly addressed, their apprehensions about personal data increase significantly. At the same time, their apprehensions increase because the speed of information diffusion on the Internet is very fast. Therefore, when incorrect information is spread, it is difficult to correct the diffused data because of the costs and time involved, as well as the lack of authority and control. The dissemination of information through retweets on Twitter and shares on Facebook, for example, is swift and widespread, and

corrections cannot be directly carried out by the data subjects when they are not the content owners. Corrections can even be difficult for content owners. Such concerns are well represented in the following responses: "I do not think I can control it" and "I want to know how my content is used, but I do not think this is possible." Therefore, worries regarding data control are readily observed online.

System/procedure Respondents also pointed out systematic and procedural reasons for deleting personal data. They fear that they will be unable to delete their data because of a lack of trust in service providers, stating, for example, "The reliability of the service is low" and "The client information on the database of the website appears when it is searched by Google, but the deletion request sent to the site administrator was not properly processed." Individual privacy leaks from Korean companies could have drawn respondents' attention to the systems and procedures of data controllers/processors. Therefore, people are apprehensive about protecting their personal data and recognize the importance of system and service reliability. Moreover, the difficulties of exerting behavior to be forgotten are repeatedly reflected in responses such as "I wanted to delete my tagged photos from Facebook but it was a photo uploaded by someone else. Untagging was the only thing I could do," "The service does not provide means or options for control," and "It is difficult to find the deletion request procedure. There is no way to contact the uploader. There is no immediate request method, such as by telephone." Such systematic factors can provide an important motive for wanting to be forgotten.

Sociality The respondents mentioned social or peer effects as a reason to delete personal data, which we call sociality. When people feel significant peer pressure from their social groups, they sometimes make decisions that are contrary to their own opinions or preferences (Udo et al. 2016). Given that people can easily know the opinions of others through online media, they can be readily influenced by them. This is reflected in their response to statements such as, "There are people with similar experiences around me" and "I see that similar things are deleted or changed by others." Some respondents have requested or have been asked to correct or delete online content: "Other people have asked me to revise or delete content." Such first-hand experiences made these respondents more cautious about uploading personal information about others and encouraged them to revise or delete their uploaded content. The motives identified and their examples of the actual quote and frequencies are summarized in Table 2, and their abstraction process is described in Fig. 1.

Additionally, respondents revealed multiple motives rather than a single motive (over 70% of respondents). In both these cases, concerns for social reputation and information disclosure are dominant (sum of the two is over 50%); these concerns are sometimes shown alone or together with other motives. Specifically, when the subject is the owner of the data, respondents show the concern for sociality or content sensitivity in addition to the concern for social reputation and information disclosure. When the subject is not the owner of the data, concerns for control over further processing, system/process, and sociality are included with the concern for information disclosure. Additionally, respondents with system/procedure concerns tend to show concern for control over further processing.

Moreover, although the frequency of each motive is somewhat similar across age and the level of Internet usage, several different patterns depend on them. For example, when the subject is the owner of the data, people in their 20 s and 30 s have more concerns for social reputation, while people in their 40 s and 50 s have more concerns for content sensitivity. When the subject is not the owner of the data, people in their 20 s and 30 s are more worried about information disclosure, while people in their 40 s and 50 s are worried about further processing. A remarkably different pattern distinguishes light users, whose Internet usage is below one hour per day. Light users are more apprehensive about control than content sensitivity. Additionally, heavy users, whose Internet usage is over six hours per day, have fewer concerns for information disclosure. This can be consistent with previous findings that less experienced users face higher uncertainty because of the absence of more domain knowledge (Taylor and Todd 1995; Hartwick and Barki 1994). Moreover, females are more apprehensive about disclosure to public or unrelated people and have fewer concerns for social reputation than males. However, there is no particular pattern across occupation.

Expected Impact of the Right to Be Forgotten on Online Content Generation

In addition to the motives for wanting to be forgotten, we asked the following question: "What changes do you see in your online content uploads if the right to be forgotten is applied?" The results of the analysis of the open-ended survey responses are mixed in terms of the expected effects of the right to be forgotten on online content generation. We first coded the responses based on positive/negative expectations and used qualitative content analysis to categorize the expected (or potential) effect, which is similar to the process to identify the motives. Positive expectations regarding the right were mentioned in the role of adjusting the imbalanced power structure between individuals and IT organizations (i.e., data controllers/processors). The respondents expected the right to be forgotten to reduce privacy concerns and encourage free expression, and thus, increasing the amount of online content. Such respondents expressed their thoughts as: "It will reduce the risk of personal information leakage,"

Table 2 Motives for deleting/revising personal data

Reason	Examples of the quotes	Subject is the owner of the data (%)	Subject is not the owner of the data (%)
Information disclosure	"I do not want my information to be made public"	236 (31.01%)	227 (26.00%)
	"I want to prevent people who are not related to me [e.g., strangers] from seeing my content"		
Content sensitivity	"The facts on [sensitive] content are wrong"	177 (23.26%)	272 (31.16%)
	"The content includes private information"		
	"Because it contains a sensitive issue"		
	"The mind or facts have changed between the time of writing and revising"		
Social reputation	"It is embarrassing to me"	197 (25.89%)	187 (21.42%)
	"It contains content that is harmful to me"		
	"It might catch up with me in the future"		
	"I am concerned about misleading information/opinions to others who see my post"		
Control over further processing	"I do not think I can control it"	78 (10.25%)	106 (12.14%)
	"I want to know how my content is used, but I do not think this is possible"		
	"It is out of control due to illegal archiving services"		
System/process	"The reliability of the service is low"	33 (4.34%)	60 (6.87%)
	"The service does not provide means or options for control"		
	"It is difficult to find the deletion request procedure. There is no way to contact the uploader. There is no immediate request method, such as by telephone"		
Sociality	"There are people with similar experiences around me"	31 (4.07%)	19 (2.18%)
	"I see that similar things are deleted or changed by others"		
	"Other people have asked me to revise or delete content"		
Others	"To improve what I have written"	9 (1.18%)	2 (0.23%)
	"I have something to fix…"		
Total		761 (100%)	871 (100%)

The numbers in columns 3 and 4 indicate frequencies and those in parentheses are the share of responses

"It will help to protect privacy," "It increases posting frequency [because] it creates safety to post," "It can lead to more freedom of expression," "It can make us share our thoughts more freely," and "Contents will be posted more if complete deletion is possible [by enforcing the right to be forgotten]." Moreover, increased control of personal data can boost individual content generation because it can be a safeguard for data control. Respondents expressed opinions such as "Information posting is likely to be done more freely because it can control the information on its own" and "I think it will have a positive impact, for example, the amount of content will increase because it will be easier to control the content I write." Additionally, some respondents mentioned that they would be more careful to respect the privacy of others when creating online content, for example, "I will be more cautious when expressing about others while writing a post" and "I will care more about privacy and respect." Lastly, respondents believe it indicates a bright Internet culture, for example, "Going to be a healthy Internet society" and "It protects the Internet browsing environment and personal information by deleting indiscriminately distributed false information." Figure 2 outlines the positive effects of the right to be forgotten on online content generation and its abstraction process.

Although many positive effects were anticipated, the negative effects of the right to be forgotten were also expected. Many respondents were concerned about abusing the right, which could result in social problems such as allowing (ex-) criminals to delete their records and facilitating information concealment and privatization. This concern was reflected in statements such as: "The original content should be saved because of concerns for social issues such as crimes," "This will make it easy for politicians and companies to privatize or conceal information," "If this makes it easy to delete, this might be more abused," and "It enables abuse by certain companies or organizations without my consent." Moreover, the respondents thought that the right to be forgotten could lead to manipulation of the press and the mass production of

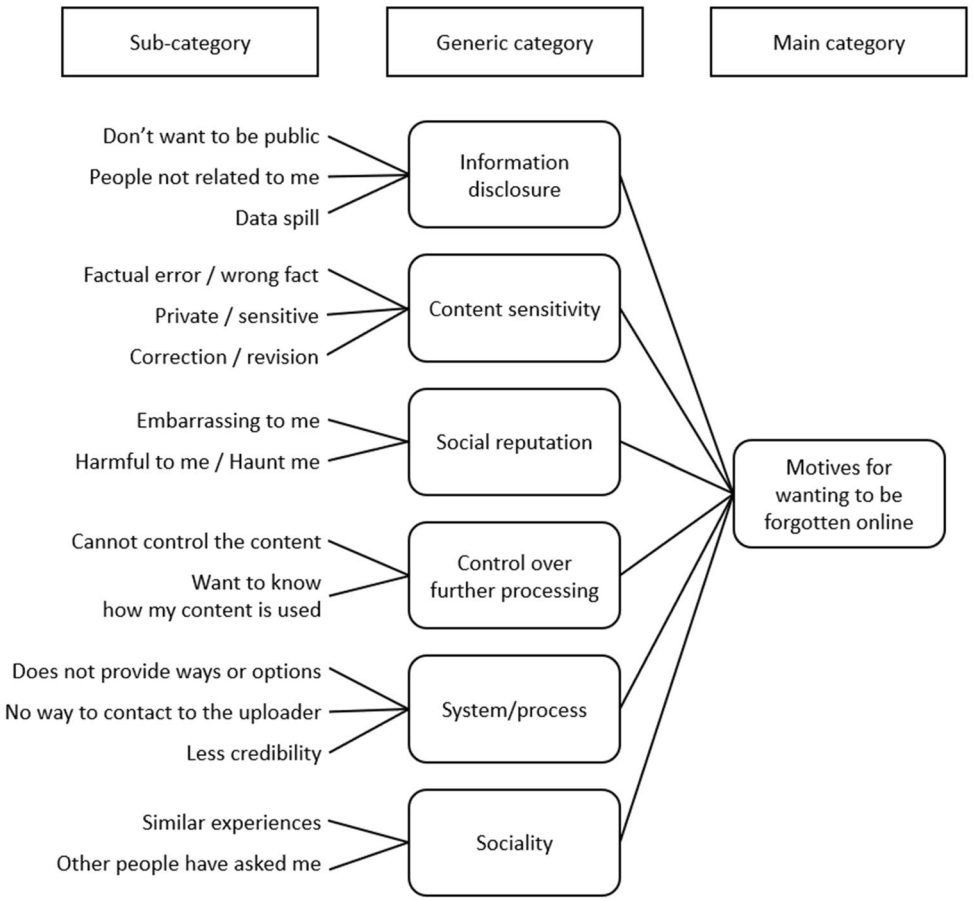

Fig. 1 An abstraction process of motives for deleting/revising personal data

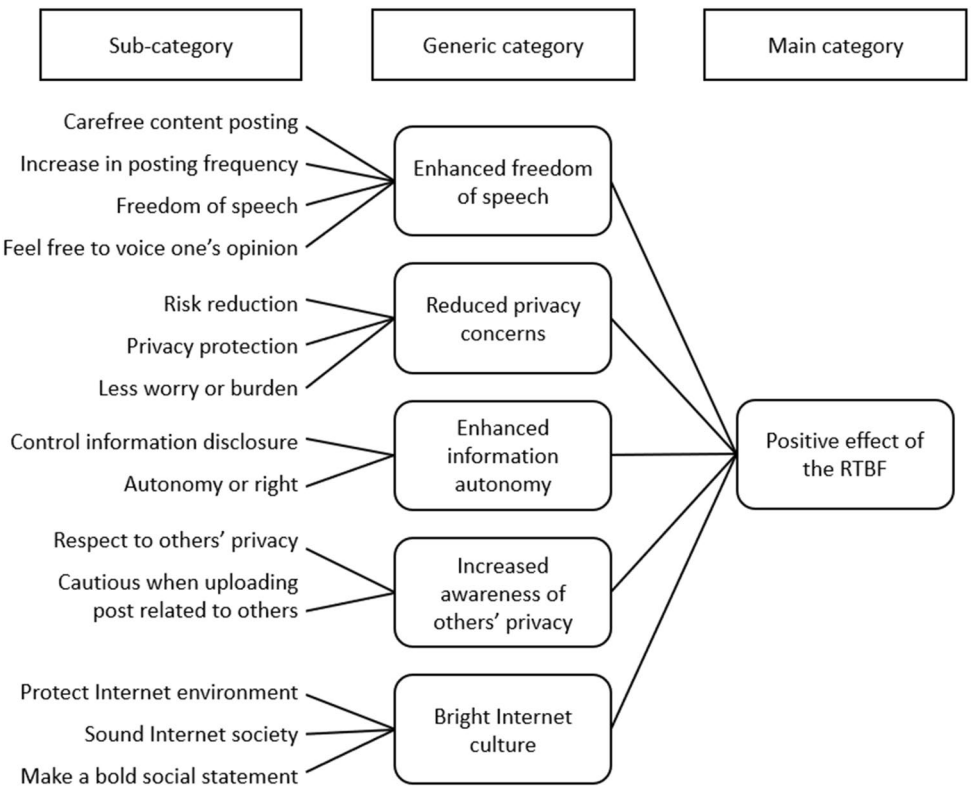

Fig. 2 Positive effects of the right to be forgotten on online content generation

false information (e.g., fake news and rumors), with diminished responsibility for information distribution. For example, "It enables artificial image [or reputation] manipulation through the misusage of RTBF," "It can lead to mass production of false information," and "It can be used to conceal facts." Additionally, they expressed the recklessness of content uploads, for example, "It encourages free registration and deletion, and increases the possibility of indiscriminate data registration [i.e., content uploads]" and "It is likely to be a more senseless posting because the content can be easily removed because of the guarantee of the right." Skeptics were also concerned about reduced freedom of speech and limited content variety. Such respondents expressed their concerns as: "Strong claims or content postings with the possibility of controversy will be reluctant," "The greater the awareness of the right to be forgotten, the more cautious is the content posting," "I think over time, only refined and simplified content will remain," and "It may cause long-term negative effects to the diversity of Internet content." The expected negative effects of the right to be forgotten on online content generation and its abstraction process are depicted in Fig. 3.

Taken together, respondents expressed the effect of the right to be forgotten as being both positive and negative. The effect might cause possible collisions between multiple rights or interests if one claimed the right to be forgotten. For example, personal interests versus social welfare, or cautious posting help support respect for others and their privacy and reduce content diversity or freedom of speech. Representatively and interestingly, although the magnitudes differ, the respondents considered the right to be forgotten both advantageous and disadvantageous to freedom of speech, depending on the context and the respondent's attitude toward digital media. Therefore, a comprehensive approach is needed rather than a piecemeal comparison to address the potential impacts of the right to be forgotten online.

Cultural Lag with the Motives Identified and Online Content Generation

The speed of social advancement is not comparable to the exponential progress of modern technology. Accordingly, the cultural lag because of the difference between the two speeds can cause ethical and privacy issues (Marshall 1999). Focusing on the cultural lag between IT and human memory, we investigate the motives for wanting to be forgotten online and its expected consequences. The results and findings of this study can help not only design privacy policies and the right to be forgotten but also reduce the cultural lag between IT and the human concept of memory. In this section, we explain how the motives identified represent a cultural lag, and an individual's need to be forgotten. We

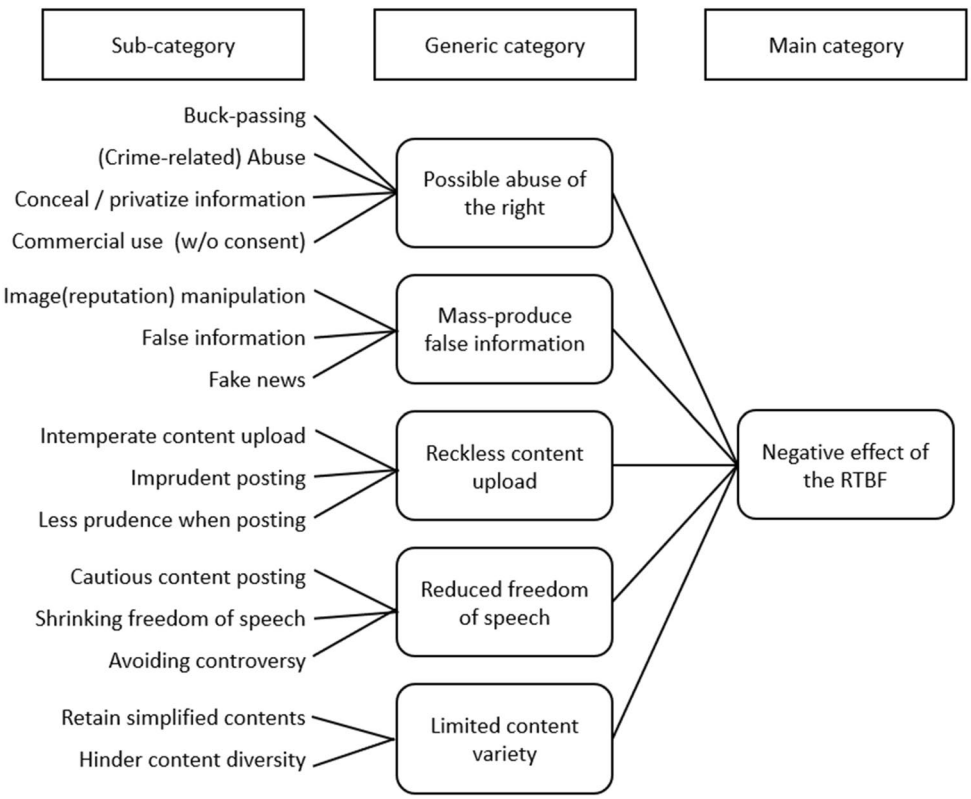

Fig. 3 Negative effects of the right to be forgotten on online content generation

adopt the framework of multidimensional developmental theory for the purpose (Laufer and Wolfe 1977). Among the elements of multidimensional developmental theory, information management covers privacy concerns regarding the management of one's personal information, whereas interaction management encompasses privacy concerns related to one's interactions with others (Hong and Thong 2013). The two categories can together provide a clearer picture of the cultural lag regarding individual privacy and how individuals perceive the lag as privacy concerns (Hoehle et al. 2018).

Some of the motives identified are included in the information management category: information disclosure, content sensitivity, control over further processing, and system/process. Disclosing personal information is a risky behavior (Belanger and Xu 2015) and the privacy literature has suggested that the decision-making processes in such behavior are affected by privacy concerns (Smith et al. 2011; Acquisti et al. 2015). However, the privacy concerns of individuals are temporary and subjective—a once fairly made privacy decision can turn out to be a bad decision in the future. Such uncertainties of individual privacy have existed for a long time; however, technological development has intensified its uncertain nature and created a great cultural lag (Marshall 1999). For example, individuals can be uncertain about whether their personal information has been disclosed to another person, groups, or the public (information disclosure) or the fact that the disclosed information is sensitive (content sensitivity) as it requires time to perceive damages due to dissemination of personal data. Digitalized data can be transferred and spread across the world in a split second and even if one realizes a bad decision has been made in the past, regretting is meaningless as the decision cannot be retracted. Furthermore, given that data do not decay, the relationship management of individuals has become time-independent, with all digitally recorded personal information being entirely managed by oneself (Howison et al. 2011). Therefore, the meanings of the two dimensions, time and range of spread, are incompatible for information providers, who feel apprehensive about their lesser control over their personal information (control over further processing) and the reliability of their communication systems (system/process).

In addition, the cultural lag can be noted in other motives in the interaction management category, namely, social reputation and sociality. Interaction management deals with how individuals manage interactions with others (Hong and Thong 2013). Individuals want to manage their social reputation by selectively disclosing their personal information (social reputation), and occasionally responding to the requests or behaviors of others (sociality). Additionally, as information disclosure is a type of basic behavior to initiate various types of relationships (Sprecher and Hendrick 2004; Wheeless and Grotz 1976), the motives for information disclosure are also considered in the interaction management category. Personal interactions in the past remained personal so that only the persons directly involved were aware of them. However, in the age of the Internet, the social interactions of individuals can easily surpass expectations in terms of time and range of spread. Even intimate conversations between family members or lovers can be publicized or leaked online, and hence, might be harmful to the reputation of others (Cukier and Mayer-Schoenberger 2013). Having observed such leaks, individuals might desire to acquire the ability to manage social relationships on their own and mitigate privacy concerns.

Additionally, the dominance of social reputation and information disclosure might indicate that respondents revealed the motive for both categories of privacy concerns (i.e., information management and interaction management). Moreover, the prevalence of multiple motives expressed by respondents also indicates their multiple privacy concerns. While their tendency to raise the concern for information management was greater, they generally demonstrated privacy concerns simultaneously for both information and interaction management. The co-occurrences of motives can be interpreted as an indication of complexity in wishing to be forgotten and resolving privacy issues. In other words, addressing multiple aspects of concerns is necessary to handle the privacy issues of wanting to be forgotten. Additionally, individuals can interpret cultural lag differently according to the social sub-groups to which they belong (Shahin 2016). The results suggest that individuals' motives for longing to be forgotten can be affected by age, Internet usage, and gender, and provide a plausible explanation of this tendency. While this study provides a cornerstone for the role of social sub-groups in the interpretation of the right, our findings are limited to some demographics and the overall Internet usage amount. Additional studies considering other factors such as more detailed Internet usage patterns or contextual aspects are necessary to broaden the understanding.

From the motives identified and related discussions, we posit that the cultural lag impacts various aspects of an individual's privacy, including information management and interaction management. Therefore, reducing a single aspect of such concerns might not result in resolving individuals' apprehensions about wanting to be forgotten and the cultural lag. A social effort could be undertaken, using the right to be forgotten as a comprehensive solution, to reduce the cultural lag regarding privacy. When the right to be forgotten is appropriately implemented in addition to the fulfillment of the above-mentioned motives, individuals could enjoy several benefits of online content generation resulting from the reduced lag. For instance, individuals' freedom of speech can be enhanced and freer opinions on the Internet will be possible because one's online content can be retrieved as one wishes. Some of the motives, including

information disclosure and control over further processing, may dissuade individuals from generating online content and sharing information with others. When the right can effectively protect their privacy, the less-burdened individuals can generate online content more actively and add diversity to online society. Furthermore, the right can alert individuals that the privacy of others is as important as their own because the same regulation for privacy can be applied to all the members of society. However, the right to be forgotten also has negative aspects. When the right to be forgotten is abused, the Internet can become overwhelmed by spontaneous and temporal data that is valid only for a short period. These data and contents aggravate the Internet environment by mass production of false information, recklessly uploaded contents, and a deluge of information. Thus, individuals could experience reduced freedom of speech because of fears of being accused of uploading content that might or might not be true. Therefore, conflicts between diverse rights, motives, and effects can cause other or even more complex problems. We note that the motives for longing to be forgotten have favored individuals, implying that their evaluations are inclined to their own interests. However, that does not necessarily mean that such interests are superior to any other interests. The definition of the right to be forgotten clearly states the necessity of balancing between multiple interests (European Parliament 2016). We hope that the identified motives and expected results of the right can lead to further discussions to determine a better implementation form of the right.

Together, an understanding of the motives for wanting to be forgotten and the effects of guaranteeing it is critical in the design of the right to be forgotten and the reduction of the cultural lag. As the motives for wanting to forgotten online that were identified in this study describe privacy concerns created or amplified by the lag, design and direction of the right to be forgotten need to consider the motives to reduce the lag. The expected effects of the right to be forgotten are helpful for its design; for example, positive expectations can guide the direction and objectives of implementing the right, while negative expectations can caution against potential side effects. The motives and expectations of individuals regarding privacy and the right to be forgotten must be considered in the right's design and its implementation to truly make social adjustments and create consensus and eventually reduce the cultural lag.

Implications

In this study, we offer several implications for research bodies. First, we show that the existence of the cultural lag is reflected in individuals' motives for wanting to be forgotten online. As an early effort in revealing the motives, this study adds clarity to the delineation of the cultural lag between technology and individuals' concept of memory (Mayer-Schönberger 2011). For individuals, the Internet has become a gigantic source of memory and this radically transforms material culture with respect to individual privacy and widens the lag. Our findings can provide directions in understanding the current situation and the way ahead for reducing the lag. For this purpose, we have a unique focus of inquiry, which is the general Internet use. Previous privacy studies of motives for revising or deleting online content have mainly adopted a narrow context-based approach to investigate individual privacy, such as social network service (Sleeper et al. 2013; Wang et al. 2011). Similarly, studies have identified factors of regret behaviors on posting personal information mainly in social network contexts (Xie and Kang 2015; Dhir et al. 2016). Although it is valuable to understand and identify privacy-related motives in a certain context, there has been no investigation with the Internet as a target context. Examining the use of the Internet allows us to identify the lag between IT and the human concept of memory, generalize apprehensions about the desire to be forgotten online, and provide a direction for a better understanding of the cultural lag, individual privacy, and implementation of the right to be forgotten.

Second, this study confirms that individuals can perceive the online content of a third-party as a source of privacy concerns. Unlike many studies focusing on the situation when the uploader is the data provider, this study includes motives for wanting to be forgotten when the third-party's content contains personal information that one wants to revise or delete. This question is important as online content is easily created, shared, and reproduced irrespective of who the processor or controller is, and individuals can expect their privacy under any context based on the privacy norms of one's community (Martin and Shilton 2016). Considering one of the main purposes of the right to be forgotten is to resolve privacy issues under this very condition, this study presents an interesting implication that respondents have different motives depending on the owner of the data. When the data subject is responsible for personal data, their biggest concern is information disclosure itself. Meanwhile, when the data subject is unable to control online content, they are most worried about content sensitivity. This indicates that an individual may request to remove or delist online content for different reasons, depending on one's control over such content. This finding echoes that of Lally (1996) that the situational position of a person can influence one's privacy decision-making. Additionally, investigating the motives for wishing to be forgotten by considering both the cases of the subject being the data owner or not, this study presents the privacy needs of individuals using the Internet from a more general perspective (DeNardis 2014).

Third, by presenting motives for wanting to be forgotten and linking motives to individual privacy concerns according to the multidimensional developmental theory (Laufer and Wolfe 1977), this study expands the understanding of an individual's privacy needs. Information disclosure and content sensitivity are the main reasons for wanting to be forgotten, which are reflections of an individual's apprehensions about the situation of disclosing their information itself. Furthermore, when online content contains sensitive personal details, it terrifies individuals as they are not able to handle the situation. The major motives are closely related to the interconnected nature of the Internet, as individuals can hardly imagine control and revise digital content on the Internet because of their inability, whereas the ripple effects of privacy infringements are devastating (Garcia-Murillo and MacInnes 2018). Other motives, such as control over further processing, system/process, social reputation, and sociality, are as important as the major ones because these, too, represent some aspects of individual privacy on the Internet. An interesting finding of this study is that some motives are frequently coupled with others. For instance, the dominant motive of information disclosures can appear simultaneously with content sensitivity or sociality. This indicates not only the complexity of an individual's motive for wanting to be forgotten but also the difficulties of resolving such concerns. We call for future research on in-depth investigations on multi-layered compositions of individual privacy.

Additionally, the results reveal the effects expected of the right to be forgotten on online content generation by individuals. Although studies have pointed out the effects of guaranteeing being forgotten (Chenou and Radu 2019; Tirosh 2017), little is known about what effects users perceive and expect in practice. The effects of the right to be forgotten on freedom of speech have drawn great attention. Journalists and scholars from the concerned fields insist that the right will deteriorate overall journalism and freedom of speech (Ambrose 2014). However, the right can also improve freedom of speech for autonomy, democracy, and truth-seeking (Youm and Park 2016). This study offers mixed expectations from the individual's viewpoint. Respondents expressed both positive (increase frequency of online content generation and expressing one's opinion freely) and negative (avoiding controversies and shrunk content sharing) effects of the right on freedom of speech. We believe that further investigations on the relationship between the right and freedom of speech are necessary to find a mutual agreement in society. Additionally, increased awareness of other's privacy is worth mentioning. This expectation can be a silver lining for individual privacy because it requires participants' efforts to change not only regulations but also privacy norms of the Internet. Accordingly, the right may cause a better and brighter Internet culture in this regard. We insist that further investigations are necessary to fully understand the potential effects of the right and minimize side effects.

One might question whether respecting the desire to be forgotten is legitimate, for which we provide the following reasons. First, in terms of a right, an individual's desire to be forgotten online is closely related to one's right to pursue happiness and the right to privacy (Mantelero 2013). It is impossible to separate individuals and their data given that a significant part of their ordinary life is online. Therefore, to determine one's personal data means more than merely controlling one's intellectual property or a Facebook account (George 2017). Rather, it is the ability to define one's being and life. Hence, full control is offered to individuals when they want to provide personal data to third-party organizations as it can increase their interests. By contrast, when an individual considers retrieving personal data as a better-off option, such a decision needs to be respected for the sake of one's interests because an individual's retrieval should be as legitimate as the provision of personal data. Unfortunately, the latter has gained limited attention. We assert that, in terms of the interest of an individual, wanting to be forgotten online should be entitled to respect. Secondly, in terms of justice in distribution, we find that risks of using personal data have been solely imposed on individuals themselves. A fair allocation of both benefits and risks is the key to an equitable relationship (Singer 2000). Apparently, agreements of providing information generally specify obligations of organizations, and with one's consent, personal data can be transferred, and thus, legitimately utilized by others. When such consent expires or is canceled, the information provider hopes that precious information is deleted safely because that is the reason for which the consent was given in the first place. Individuals expect information controllers and processors to take responsibility for withdrawing personal data as much as their passion to fully utilize it (Ünal et al. 2012). Therefore, supporting the wish to be forgotten online can promote justice for the relationship between personal data providers and their counterparts.

It is another issue, however, whether one's unfulfilled interests are always legitimate. Rights and values are weighed differently according to contexts, and wanting to be forgotten online is no exception (Tavani 2018). In some cases, the aggregated social utility can overwhelm an individual's interests. For instance, if individuals' digital traces can be used to minimize the spread of the coronavirus disease of 2019, both governments and the citizens of respective countries are likely to allow active use of personal data. The context and social background should be considered to make an ethical and fair decision. Although such an approach can be criticized as "imperfect procedural justice" (Beauchamp 2001), it often produces the best achievable results in most legal systems (Robin 2009). Once the interests of different

stakeholders are identified, the interest theory of rights can help find resolutions that can maximize the responsiveness to each of the existing interests (Bharucha et al. 2006). Ultimately, balancing social values and interests can achieve a harmonious symbiosis between the well-being of individuals, enterprise activities, and social welfare. The results of this study can be a foundation on which further investigation can be initiated and developed.

To build a balanced system of personal information, our study provides insight into the three stakeholders in personal data management, namely, individuals, data controllers/processors, and governments. Individuals might not be able to evaluate the possible risks of online activities because of a lack of knowledge. They can learn about the possibility of privacy infringements and their potential consequences, however, when their online behavior involves any of the privacy concerns identified in this study. For instance, if individuals learn about the motives for social reputation and sociality, they can revisit the impulsive disclosure of intimate information. With proper knowledge about privacy, data providers can better evaluate the risk of providing personal data and carefully review the scope of the usage of private information. Additionally, they can learn that the privacy of others can be infringed upon by uploading content online. Personal data uploaded by others without proper consent can often be found, and the reckless and irresponsible creation of online content should, therefore, be prevented. Eventually, individuals must understand that the interests of others can be as important as their own.

As part of society and businesses, data controllers/processors must respect other stakeholders' interests and the common good of the society they belong to. For instance, many of the identified motives for the desire to be forgotten are directly related to data controllers/processors. Organizations must address not only legal but also individual concerns as part of their corporate responsibilities to deal with such interests of individuals (Milberg et al. 2000). Based on the identified motives, organizations can review and revise the way they utilize personal information. For example, organizations may try to assuage concerns related to motives such as control of further processing and system/procedures. To relieve such concerns, detailed user privacy options can be offered, providing various information disclosure options regarding the scope of personal data usage. They may use design elements to help individuals protect their privacy (Acquisti et al. 2017). Having channels and procedures designed to manage personal data can also help alleviate individuals' concerns. Additionally, the results imply that clarification of the terms of private information usage and their protection can mitigate individuals' privacy concerns. As many business models rely on the collection and analysis of personal information, data controllers/processors are eager to gather more data on individuals. However, they are expected to treat each individual's data responsibly and must clearly present these responsibilities to data providers. One responsibility should be to provide well-defined privacy policies for individuals and strictly follow them. Taking a further step, data controllers/processors need to confirm whether individuals fully understand the terms of agreements to provide privacy-protected relationships. Moreover, supporting the right to be forgotten could be a proactive response to safeguard against future risks as individual privacy is consistently enhanced. Preparations for wanting to be forgotten in advance can reduce costs and risks in the future.

Finally, this study can guide policymakers in establishing legal regulations on the desire to be forgotten online. First, governments are required to define a degree of information autonomy for their people. Governments must determine desirable social values within their own context (Whetstone 2001). Based on a unique value set of a social community, policymakers need to decide a socially desirable level of information autonomy and the corresponding normative guidelines (Robin 2009). Further, governments and policymakers can create privacy-friendly arenas for diverse actors given that governments have the power to set the rules of the game. Without governmental support, individuals cannot claim their privacy because of the extreme asymmetry of power. Some of the motives identified can be mitigated when governments provide safeguards and act as monitors. For example, to deal with concerns regarding system/process, governments can establish privacy auditing processes to investigate the usage of individuals' private information, so that the individuals can personally manage its scope and boundaries (Camp 2015). Furthermore, policymakers can require organizations to declare clear boundaries and purposes of using personal information to reduce concerns of further processing. This is important because the responsibilities of organizations regarding personal information are dependent on their use of personal information (Robin 2009). Another meaningful role of governments is to provide a balance between multiple parties as only they can balance multiple rights, including each individual's right to privacy and freedom of speech, with the freedom of enterprise. As far as balancing various rights are concerned, the expected effects of the right to be forgotten are worth noting. Both positive and negative effects on freedom of speech are expected, given that the right to be forgotten can produce various ripple effects on content consumption and generation. Moreover, apprehensions about the abuse of the right to be forgotten should be considered because the imprudent application of the right could cause chaos on the Internet. Therefore, clear guidelines must be provided when balancing personal interests with public needs and in setting

judicial precedents and historical records, and policymakers should address these interests carefully.

Suggestion for Future Research

This study is likely to be generalized because it focuses on a general online environmental context and potentially overlooks its idiosyncratic characteristics. In this sense, further studies in specific contexts, including services, personal data, and situations, can enhance the understanding of the right to be forgotten. Similarly, although we attempted to explain the variation based on data and found some different patterns across age, gender, and the intensity of Internet usage, there are surely other variations for the cultural lag. We call for investigations focusing on detailed dynamics of contextual compositions and cultural lags under different social settings for enriching our knowledge. Additionally, the motive of social reputation and saving face determined in this study could result from a cultural factor prevalent in Korean and East Asian contexts and the high value of saving face in Korea can affect perceptions of the right to be forgotten. The same motive might not, therefore, arise for individuals in other countries. For instance, perceived freedom of speech can be identified as a major motive for wanting or not wanting to be forgotten for individuals in the United States, which was not the case for the Koreans in this study. The perception of the right to be forgotten in the United States can differ from that in Korea. Investigations are required to identify different motives depending on different cultures and countries and how members of a society determine the legitimacy of diverse interests for implementing the right. In addition, considering the close relationship between the right and individual privacy (Mayer-Schönberger 2011), empirical evaluations of the right's effects on important factors regarding individual privacy—including users' trust and satisfaction—can add valuable insights for both researchers and practitioners of individual privacy.

Conclusion

In a hyper-connected society, different sources of information can be easily integrated and transferred. Consequently, privacy regulations and policies should encompass networks as a whole and not as fragmented pieces as only macroscopic approaches can reduce individuals' privacy concerns regarding undeletable data. The right to be forgotten can be a comprehensive approach to protecting individual privacy, which has become an unavoidable aspect of each individual's life. By revealing the motives for wanting to be forgotten, this study established a better understanding of the right to be forgotten and initiated discussions regarding this right. Moreover, the study identified the need for and range of the right to be forgotten and estimated the positive and negative effects of its implementation. These findings constitute a stepping stone in the research on individuals' right to individual privacy. In this study, we provided guidelines for practitioners, including data controllers/processors and governments.

Appendix

See Table 3.

Table 3 Full-survey Questionnaires

1.1 Have you ever revised/deleted "the content you uploaded online (posts, photos, videos, comments, etc.)"?	
If yes,	If not,
2.1 Why did you revise/delete the content you uploaded online?	3.1. Assuming you are revising or deleting the content you uploaded online (posts, photos, videos, comments, etc.), why do you think you are going to revise/delete it?
2.2 Was the revision/deletion process smooth?	3.2. Do you think you can run revise/delete smoothly?
2.3 How, if at all, was it difficult to revise/delete the content you uploaded online?	3.3. How, if at all, was it difficult to revise/delete the content you uploaded online?
4.1. Have you ever requested to revise/delete "the online content that you did not upload but was related to you (posts, photos, videos, comments, etc.)"?	
If yes,	If not,
5.1. Why did you request a revision/deletion request for the online content that you did not upload but was related to you (posts, photos, videos, comments, etc.)?	6.1. Assuming you have requested to revise/delete the online content related to you (posts, photos, videos, comments, etc.), that you did not upload, why do you want to make such a request?
5.2. Was the revision/deletion request process smooth?	6.2. Do you think it will run smoothly when you make that revision/deletion request?
5.3. How, if at all, was it difficult to request the revision/deletion of the content related to me uploaded by others?	6.3. How, if at all, was it difficult to request the revision/deletion of the content related to me uploaded by others?
7.1. How much do you know about the right to be forgotten?	
The right to be forgotten is one's right to request the removal of personal information as long as such removal does not degrade other social interests. For instance, when you Google your name, you may ask the company to delete search results that can potentially invade your privacy. Although Korea has privacy regulations for the above issues and is trying to provide autonomy to data providers, explicit legislations are still in discussion	
[This instruction is provided with questions 7.2–4. When respondents answered question 7.1, they did not see the instruction.]	
7.2. Do you think you need the right to be forgotten?	
7.3. If the right to be forgotten is enforced, at what level do you think the right to be forgotten should be enforced?	
Multiple-choice options: (1) Complete deletion of source data and its links, (2) Deletion from search results of Google, while preserving the source data, (3) Doing nothing for social interests, (4) Others (can type the text)	
7.4. What changes do you see in your online content uploads if the right to be forgotten is applied?	
Demographics	
8.1. How much time do you spend each day using the Internet (including computers and smartphones)?	
8.2. What is the average number of your daily Internet (social network sites, online community, portal, cafe, etc.) content (posts, photos, videos, comments, etc.) uploaded?	
8.3. What is the number of social media, online communities, portals, cafes, etc. that you are active on (access more than once a day)?	
8.4. What is your age range (i.e., the 20 s, 30 s, 40 s, or 50 s)?	
8.5. What is your gender?	
8.6. What is your occupation?	

Acknowledgements This research was supported by Kangnam University Research Grants (2020). We sincerely appreciate comments from the editor and anonymous reviewers.

Compliance with Ethical Standards

Conflict of interest No potential conflict of interest was reported by the authors.

References

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., et al. (2017). Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys (CSUR), 50*(3), 1–41.

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509–514.

Ambrose, M. L. (2014). Speaking of forgetting: Analysis of possible non-EU responses to the right to be forgotten and speech exception. *Telecommunications Policy, 38*(8–9), 800–811.

Ardichvili, A., Page, V., & Wentling, T. (2003). Motivation and barriers to participation in virtual knowledge-sharing communities of practice. *Journal of Knowledge Management, 7*(1), 64–77.

Beauchamp, T. L. (2001). *Philosophical ethics: An introduction to moral philosophy*. New York: Mcgraw-Hill.

Belanger, F., & Xu, H. (2015). The role of information systems research in shaping the future of information privacy. *Information Systems Journal, 25*(6), 573–578.

Bertram, T., Bursztein, E., Caro, S., Chao, H., Chin Feman, R., Fleischer, P. et al. (2019) Five years of the right to be forgotten. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, 2019* (pp. 959–972)

Bharucha, A. J., London, A. J., Barnard, D., Wactlar, H., Dew, M. A., & Reynolds, C. F., III. (2006). Ethical considerations in the conduct of electronic surveillance research. *The Journal of Law, Medicine & Ethics, 34*(3), 611–619.

Bobadilla, Á. M., & Atala, F. G. (2018). Implementation of the right to be forgotten in Chile: The right to one's image as an essential part of all people. *Journal of Information Policy, 8,* 346–361.

Brinkman, R. L., & Brinkman, J. E. (1997). Cultural lag: Conception and theory. *International Journal of Social Economics, 24*(6), 609–627.

Brose, H.-G. (2004). An introduction towards a culture of non-simultaneity? *Time & Society, 13*(1), 5–26.

Burkell, J. A. (2016). Remembering me: Big data, individual identity, and the psychological necessity of forgetting. *Ethics and Information Technology, 18*(1), 17–23.

Burnard, P. (1991). A method of analysing interview transcripts in qualitative research. *Nurse Education Today, 11*(6), 461–466.

Camp, L. J. (2015). Respecting people and respecting privacy. *Communications of the ACM, 58*(7), 27–28.

Chenou, J.-M., & Radu, R. (2019). The "right to be forgotten": Negotiating public and private ordering in the European Union. *Business & Society, 58*(1), 74–102.

Cho, J. Y., & Lee, E.-H. (2014). Reducing confusion about grounded theory and qualitative content analysis: Similarities and differences. *The Qualitative Report, 19*(32), 1–20.

Cho, H., Rivera-Sánchez, M., & Lim, S. S. (2009). A multinational study on online privacy: Global concerns and local responses. *New Media & Society, 11*(3), 395–416.

CNIL, C. N. D. L. I. E. D. L. (2015). Décision n° 2015–047 du 21 mai 2015 mettant en demeure la société GOOGLE INC (Decision No. 2015–047 of May 21, 2015 giving formal notice to GOOGLE INC.). In Retrieved from https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000030746525. Accessed 20 Aug 2020.

Cukier, K., & Mayer-Schoenberger, V. (2013). The rise of big data: How it's changing the way we think about the world. *Foreign Affairs, 92*(3), 28–40.

De Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L., & Sanchez, I. (2018). The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law & Security Review, 34*(2), 193–203.

DeNardis, L. (2014). *The global war for internet governance*. London: Yale University Press.

Dey, I. (2003). *Qualitative data analysis: A user friendly guide for social scientists*. London: Routledge.

Dhir, A., Kaur, P., Chen, S., & Lonka, K. (2016). Understanding online regret experience in Facebook use–Effects of brand participation, accessibility & problematic use. *Computers in Human Behavior, 59,* 420–430.

Dinev, T., Bellotto, M., Hart, P., Russo, V., & Serra, I. (2006). Internet users' privacy concerns and beliefs about government surveillance: An exploratory study of differences between Italy and the United States. *Journal of Global Information Management, 14*(4), 57–93.

Elo, S., & Kyngäs, H. (2008). The qualitative content analysis process. *Journal of Advanced Nursing, 62*(1), 107–115.

Erickson, P. I., & Kaplan, C. P. (2000). Maximizing qualitative responses about smoking in structured interviews. *Qualitative Health Research, 10*(6), 829–840.

European Parliament. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46. *Official Journal of the European Union (OJ), 59*(1–88), 294.

Flick, U. (2009). *An introduction to qualitative research*. Thousand Oaks: Sage.

Garcia-Murillo, M., & MacInnes, I. (2018). Così fan tutte: A better approach than the right to be forgotten. *Telecommunications Policy, 42*(3), 227–240.

George, E. J. (2017). The pursuit of happiness in the digital age: Using bankruptcy and copyright law as a blueprint for implementing the right to be forgotten in the US. *The Georgetown Law Journal, 106,* 905–932.

Gewirth, A. (1978). *Reason and morality*. Chicago: University of Chicago Press.

Gurevich, Y., Hudis, E., & Wing, J. M. (2016). Inverse privacy. *Communications of the ACM, 59*(7), 38–42.

Hartwick, J., & Barki, H. (1994). Explaining the role of user participation in information system use. *Management Science, 40*(4), 440–465.

Hoehle, H., Aloysius, J. A., Goodarzi, S., & Venkatesh, V. (2018). A nomological network of customers' privacy perceptions: Linking artifact design to shopping efficiency. *European Journal of Information Systems, 28*(1), 1–23.

Hong, W., & Thong, J. Y. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Quarterly, 37*(1), 275–298.

Howison, J., Wiggins, A., & Crowston, K. (2011). Validity issues in the use of social network analysis with digital trace data. *Journal of the Association for Information Systems, 12*(12), 767–797.

Hsieh, H.-F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative health research, 15*(9), 1277–1288.

Korea Communications Commission. (2016). *KCC takes measures to guarantee "right to be forgotten."* Gwacheon-si: Korea Communications Commission.

Lally, L. (1996). Privacy versus accessibility: The impact of situationally conditioned belief. *Journal of Business Ethics, 15*(11), 1221–1226.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues, 33*(3), 22–42.

Lowry, P. B., Cao, J., & Everard, A. (2011). Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *Journal of Management Information Systems, 27*(4), 163–200.

Malgieri, G., & Custers, B. (2018). Pricing privacy–the right to know the value of your personal data. *Computer Law & Security Review, 34*(2), 289–303.

Mantelero, A. (2013). The EU proposal for a general data protection regulation and the roots of the 'right to be forgotten.' *Computer Law & Security Review, 29*(3), 229–235.

Marshall, K. P. (1999). Has technology introduced new ethical problems? *Journal of Business Ethics, 19*(1), 81–90.

Martin, K. (2016). Understanding privacy online: Development of a social contract approach to privacy. *Journal of Business Ethics, 137*(3), 551–569.

Martin, K., & Shilton, K. (2016). Putting mobile application privacy in context: An empirical study of user privacy expectations for mobile devices. *The Information Society, 32*(3), 200–216.

Mayer-Schönberger, V. (2011). *Delete: The virtue of forgetting in the digital age*. Princeton: Princeton University Press.

Merriam, S. B. (2002). *Qualitative research in practice: Examples for discussion and analysis*. San Francisco: Jossey-Bass Inc Pub.

Milberg, S. J., Smith, H. J., & Burke, S. J. (2000). Information privacy: Corporate management and national regulation. *Organization Science, 11*(1), 35–57.

Neville, A. (2017). Is it a human right to be forgotten: Conceptualizing the world view. *Santa Clara Jounal of International Law, 15,* 157–172.

Newman, A. L. (2015). What the "right to be forgotten" means for privacy in a digital age. *Science, 347*(6221), 507–508.

Nunan, D., & Di Domenico, M. (2017). Big data: A normal accident waiting to happen? *Journal of Business Ethics, 145*(3), 481–491.
Ogburn, W. F. (1957). Cultural lag as theory. *Sociology & Social Research*, *41*, 167–174.
Padova, Y. (2019). Is the right to be forgotten a universal, regional, or 'glocal'right? *International Data Privacy Law, 9*(1), 15–29.
Rachovitsa, A. (2016). Engineering and lawyering privacy by design: Understanding online privacy both as a technical and an international human rights issue. *International Journal of Law and Information Technology, 24*(4), 374–399.
Richards, N. M., & King, J. H. (2013). Three paradoxes of big data. *Stanford Law Review Online, 66,* 41–46.
Roberts, J. A., & Wasieleski, D. M. (2012). Moral reasoning in computer-based task environments: Exploring the interplay between cognitive and technological factors on individuals' propensity to break rules. *Journal of Business Ethics, 110*(3), 355–376.
Robin, D. (2009). Toward an applied meaning for ethics in business. *Journal of business ethics, 89*(1), 139–150.
Rosen, J. (2011). The right to be forgotten. *Stanford Law Review Online, 64,* 88–92.
Rustad, M. L., & Kulevska, S. (2014). Reconceptualizing the right to be forgotten to enable transatlantic data flow. *Harvard Journal of Law & Technology, 28*(2), 349–417.
Shahin, S. (2016). Right to be forgotten: How national identity, political orientation, and capitalist ideology structured a trans-Atlantic debate on information access and control. *Journalism & Mass Communication Quarterly, 93*(2), 360–382.
Singer, M. (2000). Ethical and fair work behaviour: A normative-empirical dialogue concerning ethics and justice. *Journal of Business Ethics, 28*(3), 187–209.
Sleeper, M., Cranshaw, J., Kelley, P. G., Ur, B., Acquisti, A., Cranor, L. F., et al. (2013) I read my Twitter the next morning and was astonished: A conversational perspective on Twitter regrets. In *Proceedings of the SIGCHI conference on human factors in computing systems, 2013* (pp. 3277–3286). ACM
Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 989–1016.
Sprecher, S., & Hendrick, S. S. (2004). Self-disclosure in intimate relationships: Associations with individual and relationship characteristics over time. *Journal of Social and Clinical Psychology, 23*(6), 857–877.
Sproull, N. L. (2002). *Handbook of research methods: A guide for practitioners and students in the social sciences*. Lanham, MD: Scarecrow Press.
Strauss, A., & Corbin, J. (1990). *Basics of qualitative research* (Vol. 15). Newbury Park, CA: Sage.
Tavani, H. T. (1999). Privacy online. *ACM SIGCAS Computers and Society, 29*(4), 11–19.
Tavani, H. T. (2018). Should we have a right to be forgotten?: A critique of key arguments underlying this question. *Journal of Information Ethics, 27*(2), 26–46.
Taylor, S., & Todd, P. (1995). Assessing IT usage: The role of prior experience. *MIS Quarterly, 19*(4), 561–570.
Tesch, R. (2013). *Qualitative research: Analysis types and software*. London: Routledge.
Tirosh, N. (2017). Reconsidering the 'Right to be Forgotten'–memory rights and the right to memory in the new media era. *Media, Culture & Society, 39*(5), 644–660.
Udo, G., Bagchi, K., & Maity, M. (2016). Exploring factors affecting digital piracy using the norm activation and UTAUT models: The role of national culture. *Journal of Business Ethics, 135*(3), 517–541.
Ünal, A. F., Warren, D. E., & Chen, C. C. (2012). The normative foundations of unethical supervision in organizations. *Journal of Business Ethics, 107*(1), 5–19.
van de Kerkhof, M. (2006). Making a difference: On the constraints of consensus building and the relevance of deliberation in stakeholder dialogues. *Policy Sciences, 39*(3), 279–299.
Voss, W. G., & Castets-Renard, C. (2015). Proposal for an international taxonomy on the various forms of the right to be forgotten: A Study on the Convergence of Norms. *Journal on Telecommunications and High Technology Law, 14*(2), 281–344.
Wang, Y., Norcie, G., Komanduri, S., Acquisti, A., Leon, P. G., & Cranor, L. F. (2011). I regretted the minute I pressed share: A qualitative study of regrets on Facebook. In *Proceedings of the seventh symposium on usable privacy and security* (pp. 10): ACM
Weber, R. H. (2010). Internet of things-new security and privacy challenges. *Computer Law & Security Review, 26*(1), 23–30.
Wheeless, L. R., & Grotz, J. (1976). Conceptualization and measurement of reported self-disclosure. *Human Communication Research, 2*(4), 338–346.
Whetstone, J. T. (2001). How virtue fits within business ethics. *Journal of Business Ethics, 33*(2), 101–114.
Winslow, B. W. (2003). Family caregivers' experiences with community services: A qualitative analysis. *Public Health Nursing, 20*(5), 341–348.
Xie, W., & Kang, C. (2015). See you, see me: Teenagers' self-disclosure and regret of posting on social network site. *Computers in Human Behavior, 52,* 398–407.
Youm, K. H., & Park, A. (2016). The "right to be forgotten" in European Union Law: Data protection balanced with free speech? *Journalism & Mass Communication Quarterly, 93*(2), 273–295.