Information Systems Frontiers (2020) 22:45–57
https://doi.org/10.1007/s10796-020-09984-5

Reconciliation of Privacy with Preventive Cybersecurity: The Bright Internet Approach

Jae Kyu Lee[1,2] · Younghoon Chang[3] · Hun Yeong Kwon[4] · Beopyeon Kim[5]

Published online: 22 January 2020

Abstract
The emergence of a preventive cybersecurity paradigm that aims to eliminate the sources of cybercrime threats is becoming an increasingly necessary complement to the current self-defensive cybersecurity systems. One concern associated with adopting such preventive measures is the risk of privacy infringement. Therefore, it is necessary to design the future Internet infrastructure so that it can appropriately balance preventive cybersecurity measures with privacy protections. This research proposes to design the Internet infrastructure using the preventive cybersecurity measures of the Bright Internet, namely *preventive cybersecurity protocol* and *identifiable anonymity protocol*, and ten privacy rights derived from Europe's General Data Protection Regulations (GDPR). We then analyze the legitimacy of the five steps of the *preventive cybersecurity protocol* and the four features of the *identifiable anonymity protocol* from the perspectives of ten privacy rights. We address the legitimacy from the perspective of potential victims' self-defense rights. Finally, we discuss four potential risks that may occur to the innocent senders and proposed resilient recovery procedures.

Keywords Bright internet · Privacy rights · GDPR · Preventive cybersecurity protocol · Identifiable anonymity protocol · Self-defense rights

1 Introduction

Recently, the necessity of a preventive cybersecurity paradigm has emerged because existing self-defensive cybersecurity systems are not sufficiently secure and cybersecurity attacks are becoming more and more serious. To overcome the limitations of self-defensive systems, the preventive cybersecurity paradigm that we introduce here aims to eliminate the sources of cybercrime threats themselves. To achieve this goal, the Bright Internet architecture is proposed with five principles: (1) origin responsibility, (2) deliverer responsibility, (3) identifiable anonymity, (4) global collaboration, and (5) privacy protection (Lee 2015, 2016; Lee et al. 2018). Interestingly, the Bright Internet explicitly includes the protection of privacy as one of its principles. In the current context, the protection of privacy implies the prevention of privacy infringement that may be caused by adopting preventive cybersecurity measures.

However, a comprehensive concept of privacy rights is outlined by the General Data Protection Regulation (GDPR)

✉ Younghoon Chang
younghoonchang@bit.edu.cn

Jae Kyu Lee
jklee@kaist.ac.kr

Hun Yeong Kwon
khy0@korea.ac.kr

Beopyeon Kim
kby82@korea.ac.kr

[1] The School of Management, Xi'an Jiaotong University, No.28, Xianning West Road, Xi'an, Shaanxi 710049, People's Republic of China

[2] College of Business, KAIST, 85 Hoegiro, Dongdaemun-gu, Seoul 02455, South Korea

[3] School of Management and Economics, Beijing Institute of Technology, 5 South Zhongguancun Street, Haidian District, Beijing 100081, People's Republic of China

[4] Graduate School of Information Security, Korea University, 145 Anam-ro, Seongbuk-gu, Seoul 02841, South Korea

[5] Graduate School of Information Security, Korea University, 145 Anam-ro, Seongbuk-gu, Seoul 02841, South Korea

in Europe; its impact is global because even non-European companies accessing the private information of European citizens are subject to penalties for violating these regulations (Tikkinen-Piri et al. 2018; Mourby et al. 2018). The GDPR requires that information system designs should conform with the privacy rights of any affected organization (Tikkinen-Piri et al. 2018; Mourby et al. 2018). Similar acts become effective in California (i.e., The California Consumer Privacy Act) and by 2020 in Nevada (i.e., The Nevada Privacy Act (SB220)) (Lexology 2019). Other states' privacy bills such as those of Massachusetts (SD341), New Jersey (SB2834), Pennsylvania (HB1049), and The New York Privacy Act are still standing and waiting for the implementation in near future (Lexology 2019).

Therefore, information systems design must not only consider the needs of preventive cybersecurity but also ensure the protection of privacy rights. To fulfill these two-dimensional goals, our research proposes a framework for designing a platform capable of preventing cybersecurity attacks while also protecting individual rights to privacy. For this purpose, we adopt the protocols proposed by the Bright Internet and the privacy rights stipulated by the GDPR. It is our goal that individual organizations will be able to use this kind of platform to effectively and efficiently implement their information systems in a way that prevents cyberattacks while also protecting privacy.

Hence, we introduce the *preventive cybersecurity protocol* and the *legitimate identifiability protocol* adopted from the Bright Internet architecture and derive ten privacy rights from the GDPR. In addition, we address the situation when Internet users may voluntarily offer their private information to the trustful third party so that they can get certificate of identifiability as a base of being trusted from the unknown counterparts. For example, the credit card holders are willing to provide their personal information to the credit card companies to gain the benefit of being trusted by the merchants who will accept their credit cards. Likewise, we consider the *trust* aspect that can be supported by the Bright Internet. We also consider that the *right to self-defense of cybervictims* may supersede the privacy rights of malicious cyber attackers. For instance, the recipients of malicious e-mails who wish to prevent continued attacks can have the self-defense rights of identifying the origins and blocking them. As such, our research seeks to balance preventive cybersecurity, privacy rights, rights to self-defense, and the benefits of gaining trust using a platform such as Bright e-mail that is under development to become a foundational tool of Bright Internet (Lee 2019).

As a testbed for a preventive cybersecurity platform, we adopt the architecture of Bright Internet 1.0, which includes the *preventive cybersecurity protocol* and the *legitimate identifiability protocol.* On top of these protocols, the Bright e-mail can support innocent users who voluntarily want to guarantee the identifiability of their real name in case e-mail recipients legitimately request in order to build trustful environment with the recipients. However, they may use identifiable pseudonyms during the ordinary transaction stage to enjoy their privacy. The *preventive cybersecurity protocol* allows victims of malignant e-mails to voluntarily report the attacks to the Bright Internet Data Center, which can accumulate such data and analyze the Origin-Victim matrix, and calculate and post the Brightness Indices of spam e-mail origins. The *identifiable anonymity protocol* in the Bright Internet supports the *traceability* of origin IP address or network ID (with the option of anonymity for innocent netizens) and *legitimate identifiability* to identify the real names of malicious agents when they commit cybercrimes. However, traceability cannot be ensured merely through the application layers of the Internet using the current TCP/IPv4 protocol; hence, the Bright Internet project develops the source address validation architecture (SAVA) based protocol on the TCP/IPv6 platform to ensure traceability (Wu et al. 2007) and hacker prevention protocol to prevent being compromised. A comprehensive description of the protocols for the Bright Internet can be found in the technical report of Bright Internet 1.0 Test Bed (Lee 2019). In this paper, we limit the scope of discussion excluding cross-border issues although it would be necessary for global collaboration.

Considering the above aims, this paper proposes the preventive cybersecurity measures for designing a Bright Internet platform that can support both preventive cybersecurity measures (two protocols mentioned above) and ten privacy rights based on GDPR. Beyond this, we consider two additional associated factors: (1) the voluntary assurance of providing private information to build mutual trust and (2) the victims' rights of self-defense that may overrule the privacy rights of malicious attackers. This type of Internet platform will facilitate the implementation of preventive cybersecurity platform while securing individual's privacy.

Thus, we proceed in Section 2 by reviewing two Bright Internet preventive cybersecurity measures that are relevant to privacy rights, namely, the *preventive cybersecurity protocol* and the *identifiable anonymity protocol*. We identify five steps of the preventive cybersecurity protocol and four features of identifiable anonymity for this research purpose. Section 3 reviews the history of privacy research and derives ten privacy rights from the GDPR: (1) the right to be informed, (2) the right to access, (3) the right to rectification, (4) the right to be forgotten, (5) the right to restriction of processing, (6) the right to data portability, (7) the right to object, (8) the right to opt-out of automated systems, (9) the right not to be subjected to unsanctioned privacy invasions, and (10) the right not be known by unpermitted persons.

Section 4 reviews the literature relevant to balancing cybersecurity and privacy. We found that although there is a clear call to conduct such research, little research on this topic

has actually been conducted. Thus, we propose a research framework that considers privacy rights in conjunction with preventive cybersecurity measures. For this purpose, innocent Internet users must be distinguished from malicious attackers so that both groups can be treated differently. Section 5 identifies the risk potential of privacy-right infringements that may be invoked by the steps of the *preventive cybersecurity protocol* and the features of the *identifiable anonymity protocol*. We identify the relevant privacy rights for each step/feature and discuss whether the privacy rights of malicious attackers should be justified or overridden by the potential victims' rights of self-defense. We also evaluate the possibility of accidentally infringing upon the privacy right of innocent origins and propose a resilient recovery procedure to resume such a misunderstanding. Finally, Section 6 reviews the implications and discusses the limitations of this research and potential future research agendas.

2 Preventive Cybersecurity Measures

2.1 Cybersecurity Research Literature

Cybersecurity research in the information system community mainly studied the behavioral aspects of the individual employees (Anderson and Agarwal 2010; Wang et al. 2015; Steinbart et al. 2016; Chen and Zahedi 2016) and organizational issues (D'Arcy et al. 2009; Herath and Rao 2009; Johnston and Warkentin 2010). The research has focused more on organization and employee compliance issues, specifically on employee behaviors (Hu et al. 2012; Herath and Rao 2009; Siponen and Vance 2010; Siponen and Vance 2010). In the engineering community, the design and technology aspects of cybersecurity have been mainly studied (Lee et al. 2018).

The research in *Information Systems Frontiers* (ISF) particularly stressed the cyber risk assessment (Mukhopadhyay et al. 2019), security risk mitigation (Ye et al. 2006), IT security investment (Ezhei and Ladani 2018), information security policy (Kang and Hovav 2018), and security risk management (Lee and Lee 2012). In this regard, *ISF*'s research also focuses more on the organization and employee aspect of cybersecurity issues.

Lee (2015) has proposed the notion of origin responsibility and distinguished the importance of preventive cybersecurity, which attempts to eliminate the source of malicious emanation from the origin sites (Lee et al. 2018). To implement the preventive cybersecurity paradigm, we need to design measures that can realize the goal. The Bright Internet Project Consortium [www.brightinternet.org] is developing the Bright Internet 1.0 Test Bed as a collaboration of academic researchers and industry partners with relevant expertise in cybersecurity, e-mail, cloud services, and certification authority. The notion of preventive cybersecurity measures can be wide and diverse depending upon the type of platforms such as e-mail, web-based system, and mobile platform.

E-mail system is the most typical platform in studying the responsibility of origin and/or destination as about 90% of cybercrimes start with e-mails. Thus, the Bright Internet 1.0 Test Bed includes the development of Bright eMail and Bright Cloud as the foundational platforms. Once these platforms are built and standards are established, the extension to other platforms can be deployed without losing the consistency of technical standards.

The Bright eMail (in short, bMail) is designed to run on the *preventive cybersecurity protocol* and the *legitimate identifiability protocol.* Therefore, it is effective to explain the key features of Bright Internet by explaining these two protocols in the context of bMail. Spam e-mails are not necessarily malicious e-mails. However, most spam e-mails filtered by the inbound filtering software can be regarded as malicious from the wide sense of potential cyberattacks. Let us review here the steps of preventive cybersecurity protocol and features of legitimate identifiability (Lee 2019).

2.2 The Preventive Cybersecurity Protocol

When victims receive malicious e-mails, they can voluntarily report the incidents to the Bright Internet Data Center.

Based on accumulated reports, data related to the origin–victim (OV) matrix can be analyzed for a certain period to collect the evidence necessary to evaluate the origins of malicious e-mails. The accumulated OV matrix data can then be used to derive the Origin Brightness Indices that can be used to pressure malicious agents to reduce or cease the emanation of malicious e-mails. Figure 1 shows an overview of this process (Lee et al. 2018). The receivers may delegate the reporting role to the inbound filtering software. In this case, the filtering software should be resilient to resume accidentally filtered origins to protect the innocent origin's privacy rights as discussed in Section 5.

The steps of *preventive cybersecurity protocol* that are relevant to the privacy rights are as follows (Lee 2019):

1) *Recipient-initiated report of malicious e-mail*: The victims who receive malicious e-mails can voluntarily report such incidents to the Bright Internet Data Center. This reporting activity may be delegated to the e-mail service provider who runs the inbound filtering software by the permission of e-mail receivers.
2) *Storage of cyberattack records*: The reported records are stored in the Bright Internet Database with the receiver's permission in the form of OV matrices. In this sense, this data structure is different from the mere filtering list.

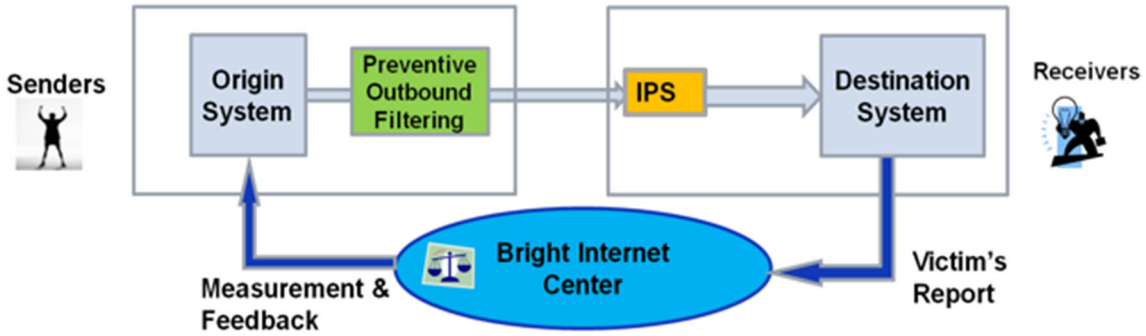

Fig. 1 Preventive Cybersecurity Protocol (Lee et al. 2018, p.67)

3) *Generating Brightness Indices of origins*: The Brightness Indices are generated by aggregating and analyzing the database in the Bright Internet Data Center.
4) *Disclosure of Brightness Indices*: Brightness Indices may be disclosed to publicize those who send malicious e-mails and to pressure them to cease emanation of malicious e-mails.
5) *Use of the Brightness Indices as filtering solutions*: The data used to generate the Brightness Indices can be used to create both inbound and outbound filtering solutions. Outbound filtering solutions are preventative solutions that would eventually reduce the risk of receiving malicious e-mails. The inbound filtering solution can be effectively customized because the Bright Internet Data Center has specific origin information.

2.3 Identifiable Anonymity Protocol

When an agent commits a cybercrime, the traceability of IP address associated with the malicious origins and identifiability of the users' real names is essential. However, it is also important to preserve the privacy of innocent users. Thus, the *principle of identifiable anonymity* in the Bright Internet (Fig. 2) aims to identify the real name of a criminal origin or equivalent identity in nearly real time when a valid search warrant was issued. However, the voluntary anonymity of innocent netizens may be preserved (Lee et al. 2018, p. 73). In this sense, we distinguish innocent users from malicious ones.

To fulfill this goal, we need to design the operation of the identifiable anonymity protocol in two steps: (1) *anonymous traceability* and (2) *legitimate identifiability* (Lee 2019). Anonymous traceability means that the IP addresses of malicious origins should be traceable with the option of permitting anonymity. For instance, the e-mail senders may retain anonymity if they do not want to publicly expose their real name. By contrast, the Bright e-mail senders may choose to guarantee the identifiability of their real names to establish trust with e-mail recipients. Thus, anonymity is a matter of choice for innocent users.

Legitimate identifiability is initiated only when cybercrime is detected by receivers and thus when an authorized agent issues a warrant of requesting the sender's real name. In GDPR, the EU treats the terms *anonymization* and *pseudonymization* as similar. However, these two terms are slightly different. Anonymization implies de-identification that is irreversible so that the personal information of the data subjects can never be identified (Mourby et al. 2018). By contrast, pseudonymization means "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately."[1] In the pseudonymization process, data controllers and processors must ensure that safeguarding and controls are in place to prevent the re-identification of personal information by unauthorized personnel.

In this regard, the *anonymous traceability* of Bright Internet can be regarded as an anonymized process as long as users are innocent. However, the identifiable anonymity protocol as a whole, including the process of legitimate identification, can be regarded as a pseudonymized process. The four feature options of the identifiable anonymity protocol are as follows (Lee 2019):

1) *Sender's voluntary disclosure of private information to gain trust* (Option 1): The e-mail receiver can trust the sender if the sender ensures identifiability as necessitated by the use of Bright eMail.
2) *Privacy protection by allowing anonymity* (Option 2): The privacy of innocent senders can be protected by allowing the anonymity.

As such, Options 1 and 2 are a matter of the sender's choice as long as the sender is innocent.

3) *Victimized recipient's ability to trace malicious senders* (Option 3): Victimized e-mail recipients may request to trace the malicious sender's IP address by an authorized

[1] Pseudonymization, GDPR Chapter 1, Article 4(5).

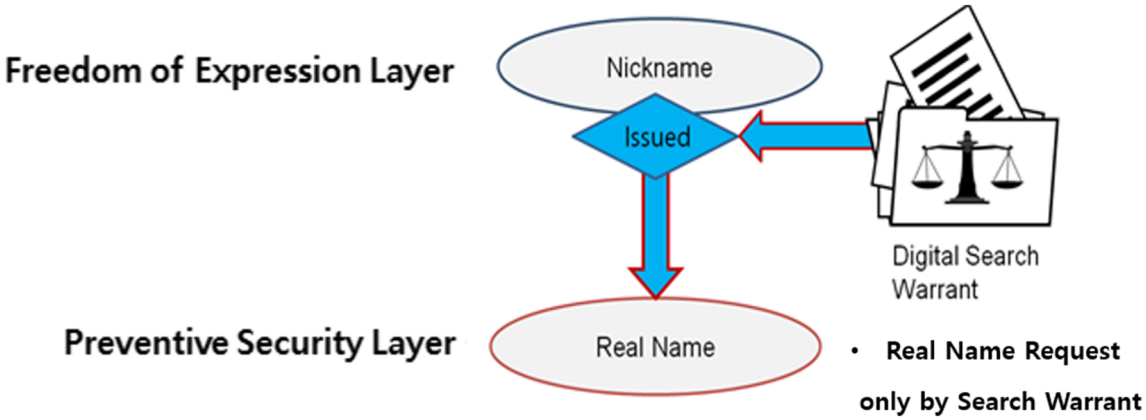

Fig. 2 Architecture of Identifiable Anonymity Protocol (Lee et al. 2018, p. 77)

agent. This request may be handled by the Bright Internet Data Center.

4) *Legitimate identifiability of malicious senders* (Option 4): Authorized agents holding search warrants may request the real-name identification of senders who committed cybercrimes.

The processes of Options 3 and 4 may cause privacy infringements of innocent senders if an innocent e-mail is misinterpreted as a cybercrime. Thus, the protocol requires a mechanism to protect against accidental privacy infringements.

3 Privacy Rights in GDPR

3.1 History of Privacy Research

Privacy is a fundamental right of individuals and constitutes a core principle of modern society. With the massive expansion of the online world, privacy issues in cyberspace have become a primary concern. Privacy concerns in cyberspace are invoked when online personal boundaries are breached or when personal information is collected and/or disseminated without permission (Adar et al. 2003). Therefore, privacy laws and regulations have arisen to protect individuals from the invasion of privacy both online and offline (Chang et al. 2018). Many fields, including management information systems, philosophy, sociology, political science, law, psychology, marketing, and economics, have published privacy studies covering topics such as the general right to privacy, general privacy as a commodity (Bélanger and Crossler 2011; Smith et al. 2011), general privacy as a state of being apart from others (Dinev et al. 2013; Westin 1967), and privacy in relation to control issues (Smith et al. 2011; Dinev 2014).

ISF's papers covered a wide range of privacy issues covering user behavior on privacy-related issues (Albashrawi and Motiwalla 2019; Ozturk et al. 2017), privacy-enhanced technologies (Loukas et al. 2012), specific technologies (Carpenter et al. 2018), and ethical issues related to privacy (Reay et al. 2013). In addition to the aforementioned topics, some papers focus on privacy policy (Singh et al. 2011; Reay et al. 2013) and GDPR (Martin et al. 2019), wherein the focus is more on the negative effect of GDPR on the startup industry. However, there were not many publications about the GDPR and its influence on cybersecurity platforms, and none yet about the preventive cybersecurity and the notion of origin responsibility.

In practice, the Fair Information Practices (FIPs) were first proposed by the US Secretary's Advisory Committee on Automated Personal Data Systems in 1973 (Breaux and Antón 2008; Elmisery et al. 2016). FIPs are characterized by five widely accepted principles: *notice*, *access*, *choice*, *security*, and *enforcement* (Wang and Emurian 2005). In the 1980s and 1990s, the Organization for Economic Cooperation and Development and the Federal Trade Commission revised the previous FIPs guidelines in response to government and business sector demands. Over the past two decades, many countries have used FIPs to develop regulation and as a foundation for national privacy policies. Among such privacy policies, the European Union's GDPR has the most comprehensive jurisdiction (Politou et al. 2018; Wachter 2018).

GDPR adopts six privacy principles: (1) lawfulness, fairness, and transparency [Article 5(1)(a)]; (2) limitations on purposes of collection, processing, and storage [Article 5(1)(b)]; (3) data minimization [Article 5(1)(c)]; (4) data accuracy [Article 5(1)(d)]; (5) data storage limits [Article 5(1)(e)]; and (6) integrity and confidentiality [Article 5(1)(f)]. Beyond these six principles, *accountability* is an additional overarching principle [Article 5(2)] that requires data custodians to guarantee compliance with all six basic principles.

3.2 Ten Privacy Rights from GDPR

For our research purposes, we derive ten privacy rights from the GDPR as owners of online personal

information (Tikkinen-Piri et al. 2018; Presthus and Sørum 2018). Beyond the eight privacy rights specified in the current GDPR guidelines, we add two more rights (Right 9 and 10) that are closely related to the preventive security paradigm of Bright Internet (EUGDPR 2018; Lee et al. 2018). The definitions of privacy rights are summarized as follows, and the sources of these rights are summarized in Table 1.

1. *Right to be informed*: Individuals have the right to know who is processing their personal data.
2. *Right to access*: Individuals have the right to access any personal data that have been collected about them.
3. *Right to rectification*: Individuals have the right to require organizations to correct inaccurate personal data.
4. *Right to be forgotten*: Individuals have the right to have their personal data deleted and to prevent further collection.

Table 1 Ten privacy rights of GDPR

Privacy rights	Relevant sources in GDPR
(R1) Right to be informed	Ch. 3, Section 2 – Information and access to personal data
	Article 13: Information to be provided when personal data are collected from the data subject
	Article 14: Information to be provided when personal data have not been obtained from the data subject
(R2) Right to access	Ch. 3, Section 2 – Information and access to personal data
	Article 15: Right of access by the data subject
(R3) Right to rectification	Ch. 3, Section 3 – Rectification and erasure
	Article 16: Right to rectification
	Article 19: Notification obligation regarding rectification or erasure of personal data or restriction of processing
(R4) Right to be forgotten	Ch. 3, Section 3 – Rectification and erasure
	Articles 17: Right to erasure ("right to be forgotten")
	Article 19: Notification obligation regarding rectification or erasure of personal data or restriction of processing
(R5) Right to restriction of processing	Ch. 3, Section 3 – Rectification and erasure
	Articles 18: Right to restriction of processing
	Article 19: Notification of obligation regarding rectification or erasure of personal data or restriction of processing
(R6) Right to data portability	Ch. 3, Section 3 – Rectification and erasure
	Articles 20: Right to data portability
(R7) Right to object	Ch. 3, Section 4 – Right to object and automated individual decision-making
	Article 21: Right to object
(R8) Right to opt-out of automated systems	Ch. 3, Section 4 – Right to object and automated individual decision-making
	Article 22: Automated individual decision-making, including profiling
(R9) Right not to be subjected to unsanctioned privacy invasion	Ch. 3, Section 5 – Restrictions
	Article 23: Restrictions
	Ch. 4, Section 5 – Codes of conduct and certificate
	Article 42: Certificate
	Article 49 (1–6): Derogations for specific situations
(R10) Right not to be known by unpermitted persons	Ch. 2 – Principles
	Article 7(1–4): Controller must get consent from data subject
	Ch. 3, Section 5 – Restrictions
	Article 23: Restrictions
	Ch. 4, Section 5 – Codes of conduct and certificate
	Article 42: Certificate

Source: https://eugdpr.org/the-regulation/

5. *Right to restriction of processing*: Individuals have the right to require organizations to restrict the processing of specific categories of personal data.
6. *Right to data portability*: Individuals have the right to require organizations to transfer personal data to a recipient of their choice.
7. *Right to object*: Individuals have the right to consent or withdraw consent concerning the processing of their personal data.
8. *Right to opt-out of automated systems*: Individuals have the right to opt-out of the use of their personal data by automated systems.
9. *Right not to be subjected to unsanctioned privacy invasion*: Individuals have the right to be left alone unless they violate laws or regulations.
10. *Right not to be known by unpermitted persons*: Individuals have the right to determine who are allowed to access their personal data and personal online space.

4 Cybersecurity and Privacy

4.1 Need to Consider Cybersecurity and Privacy in Tandem

In the academic domain, cybersecurity and information privacy issues have recently attracted much attention from IS scholars (Chang et al. 2018). Many previous studies emphasize the interrelationship between cybersecurity and privacy (Appari and Johnson 2010; Chua et al. 2017; McDaniel and McLaughlin 2009; Campbell et al. 2002; Takabi et al. 2010; Miyazaki and Fernandez 2000; Martínez-Pérez et al. 2015). For instance, Cunningham (2012) reviewed the balance between global privacy and data security laws. This issue has been addressed in the context of specific technologies, such as cloud computing (Gashami et al. 2016; Takabi et al. 2010), e-commerce (Miyazaki and Fernandez 2000), Internet of things (IoT) (Martínez-Pérez et al. 2015), medical information systems (Appari and Johnson 2010), pervasive computing (Campbell et al. 2002), and smart grid systems (McDaniel and McLaughlin 2009). These studies suggest that technologies have many security and privacy vulnerabilities that need to be addressed when developers are designing the systems.

However, few studies cover both security and privacy policy, especially in terms of the complicated legal matters involving preventive cybersecurity and privacy rights. McDaniel and McLaughlin (2009) and Takabi et al. (2010) suggest that governments should pay more attention to consumer protection and revise existing privacy and security laws. The GDPR states that data controllers or processors must ensure that they provide proper security measures, such as encryption and pseudonymization, to protect personal data.[2] These measures can prevent unauthorized parties from identifying personal information. Nevertheless, data holders still need strong security systems such as firewalls to block illegal access by unpermitted users (Mourby et al. 2018). In this regard, security schemes can contribute to the prevention of privacy infringement. However, preventive security may infringe upon personal privacy. It is therefore important to design information systems and Internet infrastructure in a way that fulfills both security and privacy goals, synergistically balancing the tradeoffs between the two.

4.2 Balancing Privacy with Cybersecurity and Trust

Even though privacy is important, it may not always be the top priority of choice. There are situations under which privacy may not be paramount: (1) legitimate preventive cybersecurity and (2) voluntary disclosure of private information to gain trust. The current research seeks to balance privacy with these factors in designing Internet infrastructures.

4.2.1 Legitimate Preventive Cybersecurity

If government agencies want to identify an individual for preventive security purposes, they require a permit and must comply with local data protection acts and regulations. However, as GDPR Article 49 states, the disclosure of personal information can be permitted when it is essential for national security, defense, public security, prosecution of criminals, and other public emergency matters.[3] The measures by the Preventive Cybersecurity Protocol can be regarded as measures for public security, because all e-mail receivers are potential victims of cyberattacks. Thus, the vulnerable e-mail receivers should have a right to self-defense against cyberattacks such as malicious e-mails. We therefore argue that the privacy of malicious e-mail senders can be overruled to ensure the safety of innocent e-mail recipients.

4.2.2 Voluntary Disclosure of Private Information to Gain Trust

Previous information privacy research, especially the privacy calculus theory, has demonstrated that an individual may be willing to disclose personal information and take risks when they perceive that their actions will yield more benefits than risks (Dinev and Hart 2006; Chang et al. 2018). In the Bright Internet context, Bright e-mail account holders voluntarily agree to be identifiable with their real names. In return, they can reap benefits associated with being implicitly trusted by unknown e-mail recipients.

[2] Pseudonymization, GDPR Chapter 1, Article 4(5).
[3] Restrictions, GDPR section 5, Article 23.

5 Privacy Rights in the Preventive Cybersecurity Measures

In this section, we analyze the five steps of preventive cybersecurity measures with the perspective of ten privacy rights to review the legal basis for the justifications. For this purpose, we study the legitimacy of the senders and receivers as summarized in Table 2. The attacked receivers/senders and Bright Internet Data Center should have the right to block the repetitive attacks and may file criminal charges and demand restitution of damages from the cyberattackers.

5.1 Privacy Rights in the Preventive Cybersecurity Protocol

For the five steps of the preventive cybersecurity protocol, we identified the privacy rights of innocent e-mail senders in Table 2. However, if the senders are malicious, we argue that receivers can have a right to self-defense against these malicious senders and that the victimized receivers thus have the right to report malicious attacks to the appropriate authorities—in this case, the Bright Internet Data Center—and delegate its generation of necessary preventive measures. Based on the delegation, the center would be permitted to

Table 2 Preventive measures, privacy rights, and analogical acts

Preventive Measures		Sender' Privacy Right		Receivers Rights
Protocols	Step	Innocent Senders	Typical Analogical Acts	
Preventive Cybersecurity Protocol	1. Report Malicious Emails	R1 (Informed) R7 (Object)	CCTV: Taking pictures	The innocent senders should have the relevant privacy rights; But the rights of malicious senders will be overruled by the receiver's self-defense right
	2. Store Malicious Emails	R4 (Forgotten)	CCTV: Storage of pictures	
	3. Generate Brightness Indices	R5 (Restrict Processing) R8 (Opt-out)	Credit information use and protection act	
	4. Disclose Brightness Indices	R4 (Forgotten)	Energy use rationalization act	
	5. Make Filtering Solution	R10 (Unpermitted)	Filtering model for the credit card authorization	
Identifiable Anonymity Protocol	1. Voluntary Disclose	None	Credit card application	Voluntary submission of private information
	2. Allowed Anonymity	R1 (Unpermitted)	Any legitimate anonymous trades	Permit the anonymity of innocent users
	3. Traceability	R1 (Unpermitted)	Investigation of prosecuted cases	Victim's right to report and criminal charge
	4. Legitimate Identifiability	R4 (Forgotten)	Surveillance acts;	Surveillance authority overrules the privacy rights of malicious senders
Privacy Protection of Innocent Sender	1. Accidental False Report	R1 (Informed) R2 (Access) R3 (Rectify) R4 (Forgotten)	Recovery procedure	Resume the privacy rights resiliently
	2. Intentional False Report	R1 (Informed) R2 (Access) R3 (Rectify R4 (Forgotten)	Recovery procedure	Resume the privacy rights resiliently, and senders may make criminal charges
	3. Compromised Senders	R1 (Informed) R2 (Access) R3 (Rectify)	Prevent being compromised by adopting the Hacker Prevention Protocol	Compromised attackers are distinguished from malicious origin, but have the deliverer responsibility
	4. Abused Request of Identification	R4 (Forgotten)	Audit trail an recovery procedure	Abused request of identification should be withdrawn and resume the privacy rights

store the reports, generate and disclose the Brightness Indices, and create and distribute the preventive cybersecurity solutions using the indices. These actions would contribute to preventing repetitive cyberattacks against innocent e-mail recipients.

In this case, the privacy rights of malicious agents can be overruled because the victim's right to self-defense against cyberattacks in the form of malicious e-mail should have a higher priority. Thus, the actions of Bright Internet Data Center would be legitimate as long as the Bright e-mail system and the Bright Internet Data Center clearly post their policy and confirm that reporting receivers agree to the policy. We review the potential privacy rights of innocent senders for each step, discuss the rights to self-defense, and demonstrate analogous laws that share the common legal spirit.

1) *Recipient-initiated report of malicious e-mails:* In this step, the reported senders have the "right to be informed" and "right to object," but the malicious sender's rights can be overruled to protect the victim's right to self-defense. An analogous case is the preventive function of a CCTV system that permits recording private information in public or private vehicles so that individuals can be traced in case of criminal activity. However, the records about innocent citizens should be protected, but when a crime is detected, police can legitimately trace the origin of crime. Likewise, innocent e-mails will not be reported, only the malicious ones.
2) *Storage of cyberattack records*: The reported senders have the "right to be forgotten," but the malicious senders' right can be overruled to preserve the victim's right to self-defense. Storing a CCTV record for a reasonable period is an analogical example. The government may require the certification of Bright Internet Data Center to assure its public role. To prevent the misuse of stored data during the operation stage, it will be necessary to maintain an audit trail, which could, perhaps, be implemented by the Blockchain technology.
3) *Generating Brightness Indices*: The generation of Brightness Indices is relevant to the "right to restrict processing" and the "right to opt-out of automated systems." However, these rights of malicious senders can be overruled to ensure the capability of identifying potential cyberattackers. Similar laws already allow the generation of credibility information for preventive measures. For example, in Korea, the Act on the Consumer Protection in Electronic Commerce [Article 27 and 28], Credit Information Use and Protection Act [Article 15], Financial Investment Services and Capital Markets Act [Article 335(11)], and Regulations on Financial Investment Services permit to compute the credibility information. Analogous rules that permit similar analysis include the Framework Act on Food Safety in Korea [Article 24(1)] and an energy efficiency rating system of electronic devices.
4) *Disclosure of Brightness Indices*: Disclosing the Brightness Indices of Origins is relevant to the "right to be forgotten." GDPR Articles 33 and 34 address disclosure by requiring giving notice to and communicating with data subjects. However, we argue that the right of malicious senders can be overruled because the purpose of disclosure is to share preventive information with potential victims and demotivate the emanation of malicious e-mails. However, organizations with high Brightness Indices can leverage public disclosure, thereby gaining trust and improving their reputations. A similar legislation in Korea is the Energy Use Rationalization Act [Article 15(1)] that requires a publicly displayed rating system. In the USA, public disclosure of sex offenders is required as a means of preserving public safety and preventing repeat offenses according to the Act on the Protection of Children and Youth against Sex Offenses [Article 49].
5) *Use of the Brightness Indices as filtering solutions*: Generation of filtering solutions using the index information may infringe upon the "right not to be known by unpermitted persons." However, the right of malicious senders should be overruled to prevent the repetitive malicious behavior that can harm the potential e-mail receivers. This is analogous to sharing the misbehavior information of credit holders with all merchants during the authorization process. A related law is the Framework Act on the Safety of Products in Korea [Article 15(2)], which allows for access to information if consumers have concerns about product safety.

Overruling the privacy rights of malicious e-mail senders in a similar context seems legitimate because it contributes to the prevention of repetitive threats to victims and potential victims. As such, preventive cybersecurity measures can be legitimized as the self-defensive actions of potential victims. Each country may need to review this issue from the perspective of their own laws, but it seems commensurate with similar laws in many countries.

5.2 Privacy Right in Identifiable Anonymity Protocol

The privacy issues in four features of the *identifiable anonymity protocol* are the following.

1) *Sender's voluntary disclosure of private information to gain trust* (Option 1): An e-mail sender may voluntarily assure its identifiability to gain the trust from the counterparts in cyberspace. Therefore, in this case, no potential risk of privacy infringement occurs.

2) *Privacy protection by allowing anonymity* (Option 2): As long as an individual does not commit cybercrime (including sending malicious e-mails), the Bright Internet platform allows the users' anonymity. This principle supports the realization of the "right not to be known by unpermitted persons." Any legitimate anonymous trades in our daily lives correspond to this practice.
3) *Traceability of malicious e-mails* (Option 3): Innocent senders should have the "right of not to be known by unpermitted persons." However, any recipients of malicious e-mails should be authorized to request tracing the sender's IP address, based on the right of self-defense. However, the actual investigation should be performed by legally authorized agencies in cooperation with a delegated operator such as the Bright Internet Data Center. This corresponds to the investigation of prosecuted crimes.
4) *Legitimate identifiability of malicious senders* (Option 4): The legitimate request for the real name of malicious senders can be regarded as a legitimate investigation process according to GDPR Article 49 (1–6) on derogations for specific situations. In the USA, the Electronic Communications Privacy Act of 1986 (Rosenstein 1991) and the Foreign Intelligence Surveillance Act of 1978 support the right to investigate malicious acts. The United Kingdom's Regulation of Investigatory Power Act of 2000 (Article 28) also supports such investigation as a means of self-defense or a justifiable act (Lin 2016).

For innocent users, privacy rights are supported in Options 1 and 2. However, for malicious actors, privacy rights are overruled in Options 3 and 4.

5.3 Privacy Protection for Innocent Origins

So far, we have primarily analyzed the cybersecurity and privacy rights from an e-mail recipient's point of view. However, four types of potential errors may occur even in the Bright Internet context: accidental false report, intentional false report from malicious e-mail recipients, compromised senders, and misuse of the request for origin's identification. The Bright Internet should be designed to be resilient to these occurrences.

1) *Accidental false report from innocent e-mail recipient*: The automatic filtering solution may make this kind of mistake, so the recovery procedure should be equipped with friendly interaction. In this case, the potentially innocent sender should be informed, the stored data should be accessible, and the incorrect report should be rectified. The Bright Internet Data Center should send a confirmation e-mail to the sender to confirm the "right to be informed" and "right to access." If a mistake on the part of the e-mail recipient is confirmed, the innocent e-mail sender should be provided with the "right to rectification" and the "right to be forgotten," and the record should be corrected accordingly.
2) *Intentional false report from malicious e-mail recipient*: This would be a reverse malicious attack against an innocent e-mail sender if the hackers compromise the receiver's computer. This would be unlikely to happen in the properly developed Bright eMail systems with the capability of the hacker prevention protocol. However, unpredictable attacks may happen. If hackers were able to penetrate the receiver's system and harm an innocent e-mail senders and the Bright Internet Data Center itself, the innocent sender should be able to report the attack to the center so that the wrong records could be confirmed and deleted with the protection offered by the "right to be informed," "right to access," "right to rectification," and "right to be forgotten." The Bright Internet Data Center should be equipped with the ability to protect and recover the innocent e-mail senders. The center and attacked senders would have the right to make criminal charges and demand restitution of damages from the cyberattackers.
3) *Compromised senders*: When a sender's e-mail account is compromised, the sender is also a victim. As such, compromised senders should be protected through the "right to be informed", "right to access," and the "right to rectification." However, the compromised computers also have the delivery responsibility as neighbor (Lee et al. 2018); thus, their records of compromised attackers cannot be deleted. Therefore, the compromised senders should do their best not to be compromised by using a hacker prevention protocol that prevents hackers from compromising e-mail accounts. Users who do not diligently adopt such a preventive system should bear the relevant responsibility of becoming an instrument of the attack.
4) *Abused request for identification*: Identification requests for real names may be abused accidentally or intentionally. To prevent privacy infringement caused by such misuse, the identification process should be recorded and securely logged to ensure its auditability. If an e-mail sender turns out to be innocent after the process of legitimate identifiability, the "right to be forgotten" should be guaranteed.

6 Conclusion

We have reviewed the legitimacy of Bright Internet preventive cybersecurity measures in conjunction with the privacy rights requested by the GDPR. For the five steps of the *preventive*

cybersecurity protocol (reporting malicious e-mails, storing the records of malicious e-mails, generating Brightness Indices, disclosing Brightness Indices, and creating a filtering solution using the indices), it seems that the victim's right to self-defense can overrule the privacy rights of malicious senders summarized in Table 2. Laws in other security contexts such as CCTV, credit information use and protection, disclosure of energy efficiency, and credit card authorization model are demonstrated as evidence of balancing between preventive measures against malicious attackers and privacy rights of innocent e-mail senders.

The *identifiable anonymity protocol* defines the situations when the e-mail senders may voluntarily disclose their private information to establish trust with unknown e-mail recipients, and innocent e-mail users may also choose to use anonymity, invoking their "right not to be known by unpermitted persons." In this context, privacy is a matter of user's choice. However, when the victims are attacked and are vulnerable to repetitive attacks in the future, they should have the right to request tracing and identifying the sender's real names to legal agency. In this case, the prosecution and surveillance authorities will overrule the privacy rights of malicious agents.

Finally, the potential risks that innocent senders may face and resilient recovery requirements are described. For instance, false reports from receivers may be submitted to the Bright Internet Data Center accidentally by spam filtering solutions or intentionally by hackers. In these cases, the Bright Internet platform should be equipped with the effective recovery of innocent sender's privacy rights. Another case of innocent senders is the compromised malicious senders. They are also victims, but they should take the responsibility of not being compromised and not becoming the instrument of hacker's attacks. Hence, they should be diligently equipped with the hacker prevention protocol. Finally, the innocent senders may be victimized by the abused request of identification. Therefore, the audit trail is necessary to demotivate such requests possibly by implementing a Blockchain technology.

Through this study, we have justified the legitimacy of preventive cybersecurity measures in the Bright Internet protocols. However, we also have identified four new potential problems that the Bright Internet protocols may face and proposed how to recover when it happens. Thus, we have extended the view of balancing the preventive cybersecurity measures with assuring the privacy of e-mail receivers and senders.

Currently, specific legislation that balances preventive cybersecurity with privacy rights has not been specifically enacted in most countries. However, our analysis shows that it seems possible to legitimately adopt the preventive cybersecurity measures in conformity with the individual privacy rights based on the common spirit of existing laws in many countries.

References

Adar, E., Lukose, R., Sengupta, C., Tyler, J., & Good, N. (2003). Shock: Aggregating information while preserving privacy. *Information Systems Frontiers, 5*(1), 15–28.

Albashrawi, M., & Motiwalla, L. (2019). Privacy and personalization in continued usage intention of mobile banking: An integrative perspective. *Information Systems Frontiers, 21*(5), 1031–1043.

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly, 34*(3), 613–643.

Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: Current state of research. *International Journal of Internet and enterprise management, 6*(4), 279–314.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly, 35*(4), 1017–1042.

Breaux, T., & Antón, A. (2008). Analyzing regulatory rules for privacy and security requirements. *IEEE Transactions on Software Engineering, 34*(1), 5–20.

Campbell, R., Al-Muhtadi, J., Naldurg, P., Sampemane, G., & Mickunas, M. D. (2002). Towards security and privacy for pervasive computing. In *International Symposium on Software Security* (pp. 1-15). Springer, Berlin, Heidelberg.

Carpenter, D., McLeod, A., Hicks, C., & Maasberg, M. (2018). Privacy and biometrics: An empirical examination of employee concerns. *Information Systems Frontiers, 20*(1), 91–110.

Chang, Y., Wong, S. F., Libaque-Saenz, C. F., & Lee, H. (2018). The role of privacy policy on consumers' perceived privacy. *Government Information Quarterly, 35*(3), 445–459.

Chen, Y., & Zahedi, F. M. (2016). Individual's internet security perceptions and behaviors: Polycontextual contrasts between the United States and China. *MIS Quarterly, 40*(1), 205–222.

Chua, H. N., Wong, S. F., Chang, Y., & Libaque-Saenz, C. F. (2017). Unveiling the coverage patterns of newspapers on the personal data protection act. *Government Information Quarterly, 34*(2), 296–306.

Cunningham, M. (2012). Privacy in the age of the hacker: Balancing global privacy and data security law. *George Washington International Law Review., 44*(4), 643–696.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20*(1), 79–98.

Dinev, T. (2014). Why would we care about privacy? *European Journal of Information Systems, 23*(2), 97–102.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61–80.

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-

related concepts. *European Journal of Information Systems, 22*(3), 295–316.
Elmisery, A. M., Rho, S., & Botvich, D. (2016). A fog based middleware for automated compliance with OECD privacy principles in internet of healthcare things. *IEEE Access, 4*, 8418–8441.
EUGDPR. (2018). The EU General Data Protection Regulation. https://eugdpr.org/the-regulation/. Accessed 21 June 2019.
Ezhei, M., & Ladani, B. T. (2018). Interdependency analysis in security investment against strategic attacks. *Information Systems Frontiers*, 1–15. https://doi.org/10.1007/s10796-018-9845-8.
Gashami, J. P. G., Chang, Y., Rho, J. J., & Park, M. C. (2016). Privacy concerns and benefits in SaaS adoption by individual users: A trade-off approach. *Information Development, 32*(4), 837–852.
Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154–165.
Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences, 43*(4), 615–660.
Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly, 34*(3), 549–566.
Kang, M., & Hovav, A. (2018). Benchmarking methodology for information security policy (BMISP): Artifact development and evaluation. *Information Systems Frontiers*, 1–22.
Lee, J. K. (2015). Research framework for AIS grand vision of the bright ICT initiative. *MIS Quarterly, 39*(2), iii–xii.
Lee, J. K. (2016). Invited commentary reflections on ICT-enabled bright society research. *Information Systems Research, 27*(1), 1–5.
Lee, J. K. (2019), Technical report of architecture of bright internet 1.0 test bed, unpublished working paper with bright eMail capability, work-in-progress.
Lee, J. K., Cho, D., & Lim, G. G. (2018). Design and validation of the bright internet. *Journal of the Association for Information Systems, 19*(2), 63–85.
Lee, M., & Lee, J. (2012). The impact of information security failure on customer behaviors: A study on a large-scale hacking incident on the internet. *Information Systems Frontiers, 14*(2), 375–393.
Lexology (2019). New State Bills Inspired by the California Consumer Privacy Act May Re-appear Next Year. Ropes & Gray LLP (November 7, 2019). https://www.lexology.com/library/detail.aspx?g=46f5bb8e-ae93-45e6-b287-f771a6b751af. Access 30 November 2019.
Lin, Patrick. (2016). Ethics of hacking Back: Six arguments from armed conflict to zombies, ethics+emerging sciences group.
Loukas, A., Damopoulos, D., Menesidou, S. A., Skarkala, M. E., Kambourakis, G., & Gritzalis, S. (2012). MILC: A secure and privacy-preserving mobile instant locator with chatting. *Information Systems Frontiers, 14*(3), 481–497.
Martin, N., Matt, C., Niebel, C., & Blind, K. (2019). How data protection regulation affects startup innovation. *Information Systems Frontiers*, 1–18. https://doi.org/10.1007/s10796-019-09974-2,21.
Martínez-Pérez, B., De La Torre-Díez, I., & López-Coronado, M. (2015). Privacy and security in mobile health apps: A review and recommendations. *Journal of Medical Systems, 39*(1), 181.
McDaniel, P., & McLaughlin, S. (2009). Security and privacy challenges in the smart grid. *IEEE Security & Privacy, 7*(3), 75–77.
Miyazaki, A. D., & Fernandez, A. (2000). Internet privacy and security: An examination of online retailer disclosures. *Journal of Public Policy & Marketing, 19*(1), 54–61.
Mourby, M., Mackey, E., Elliot, M., Gowans, H., Wallace, S. E., Bell, J., et al. (2018). Are 'pseudonymised'data always personal data? Implications of the GDPR for administrative data research in the UK. *Computer Law & Security Review, 34*(2), 222–233.
Mukhopadhyay, A., Chatterjee, S., Bagchi, K. K., Kirs, P. J., & Shukla, G. K. (2019). Cyber risk assessment and mitigation (CRAM) framework using logit and probit models for cyber insurance. *Information Systems Frontiers, 21*(5), 997–1018.
Ozturk, A. B., Nusair, K., Okumus, F., & Singh, D. (2017). Understanding mobile hotel booking loyalty: An integration of privacy calculus theory and trust-risk framework. *Information Systems Frontiers, 19*(4), 753–767.
Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity, 4*(1), tyy001.
Presthus, W., & Sørum, H. (2018). Are consumers concerned about privacy? An online survey emphasizing the general data protection regulation. *Procedia Computer Science, 138*, 603–611.
Reay, I., Beatty, P., Dick, S., & Miller, J. (2013). Privacy policies and national culture on the internet. *Information Systems Frontiers, 15*(2), 279–292.
Rosenstein, S. (1991). Electronic Communications Privacy Act of 1986 and Satellite Descramblers: Toward Preventing Statutory Obsolesence. *Minnesota Law Review, 76*, 1451–1481.
Singh, R. I., Sumeeth, M., & Miller, J. (2011). A user-centric evaluation of the readability of privacy policies in popular web sites. *Information Systems Frontiers, 13*(4), 501–514.
Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly, 34*(3), 487–502.
Smith, J. H., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 989–1015.
Steinbart, P. J., Keith, M. J., & Babb, J. (2016). Examining the continuance of secure behavior: A longitudinal field study of mobile device authentication. *Information Systems Research, 27*(2), 219–239.
Takabi, H., Joshi, J. B., & Ahn, G. J. (2010). Security and privacy challenges in cloud computing environments. *IEEE Security & Privacy, 8*(6), 24–31.
Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU general data protection regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review, 34*(1), 134–153.
Wachter, S. (2018). Normative challenges of identification in the internet of things: Privacy, profiling, discrimination, and the GDPR. *Computer law & security review, 34*(3), 436–449.
Wang, J., Xiao, N., & Rao, H. R. (2015). An exploration of risk characteristics of information security threats and related public information search behavior. *Information Systems Research, 26*(3), 619–633.
Wang, Y. D., & Emurian, H. H. (2005). An overview of online trust: Concepts, elements, and implications. *Computers in Human Behavior, 21*(1), 105–125.
Westin, A. F. (1967). *Privacy and freedom*. New York: Atheneum.
Wu, J., Ren, G., & Li, X. (2007). *Source address validation: Architecture and protocol design* (pp. 276–283). Beijing: IEEE International Conference on Network Protocols.
Ye, N., Farley, T., & Lakshminarasimhan, D. (2006). An attack-norm separation approach for detecting cyber attacks. *Information Systems Frontiers, 8*(3), 163–177.

Jae Kyu Lee is the Distinguished Professor of School of Management at Xi'an Jiaotong University and Professor Emeritus of Korea Advanced Institute of Science and Technology (KAIST). He has been professor of KAIST since 1985, and finished his tenure as HHI Chair Professor. He is a fellow and was the President (2015-6) of Association for Information

Systems, the global organization of 4,000 Information System researchers. He is the founder of Principles for the Bright Internet and founded Bright Internet Research Center at KAIST and Xi'an Jiaotong University. He also founded the Bright Internet Global Summit (BIGS) 2017 in Seoul, Korea and co-chaired BIGS2018 at San Francisco in the USA and BIGS2019 at Munich in Germany. He founded the Bright Internet Project Consortium in 2019 as posted at www.brightinternet.org. He received his Ph.D. in Information and Operations Management from the Wharton School, University of Pennsylvania in 1985.

Younghoon Chang is an Associate Professor and a Doctoral Supervisor in the School of Management and Economics at Beijing Institute of Technology, Beijing, China. He received his Ph.D. degree in Business & Technology Management from Korea Advanced Institute of Science and Technology (KAIST), South Korea. His research interests include information privacy, privacy policy & regulation, IT user behavior, shared economy, crowdsourcing, and smart health. His articles have appeared in Information Systems Frontiers, Information & Management, Government Information Quarterly, Journal of Global Information Management, Behavior and Information Technology, Industrial Management & Data Systems, Telecommunications Policy as well as in the proceedings of international conferences. He is currently serving as an associate editor of Asia Pacific Journal of Information Systems and an editorial review board member of Journal of Computer Information Systems.

Hun Yeong Kwon is a Professor of Graduate School of Information Security at Korea University since 2015. He was a professor in the College of Law at the Kwangwoon University from 2008 to 2015. Having majored in administrative and ICT laws, and he has worked for the Korean government and the academic community for the last 20 years on informatization and ICT of Korea as well as the legal framework for e-government. He is a president of the Cyber Communication Academic Society in Korea, and he was a president of the Korea Society of Internet Ethics from 2017 to 2018.

Beopyeon Kim is a Ph.D. candidate and a researcher at the Center for Cyber Security Policy of Korea University. Having majored in administrative and ICT laws, and area of research interests are Law and Policy for Information Security, Law on Internet, and Law on Privacy. She received a Master Degree in Law from Kwangwoon University in 2014. She has worked the Korean Education Development Institute in 2014 as a researcher and had a researcher of the Korean Institute of Intellectual Property in 2016.