Journal of the Association for Information Systems (2018) **19**(2)**,** 63-85
doi: 10.17705/1jais.00484

EDITORIAL

ISSN 1536-9323

Design and Validation of the Bright Internet

Jae Kyu Lee[1], Daegon Cho[2], Gyoo Gun Lim[3]

[1] KAIST, Yonsei University, Carnegie Mellon University, Xi'an Jiaotong University, jklee@kaist.ac.kr
[2] College of Business, KAIST, daegon.cho@kaist.ac.kr
[3] School of Business, Hanyang University; gglim@hanyang.ac.kr

Abstract

Bright Internet research was launched as a core project of the AIS Bright ICT Initiative, which aims to build an ICT-enabled Bright Society. To facilitate research on the Bright Internet, we explicitly define the goals and principles of the Bright Internet, and review the evolution of its principles. The three goals of the Bright Internet are: the realization of preventive security, the provision of the freedom of anonymous expression for innocent netizens, and protection from the risk of privacy infringement that may be caused by preventive security schemes. We respecify design principles to fulfill these seemingly conflicting goals: origin responsibility, deliverer responsibility, identifiable anonymity, global collaboration, and privacy protection. Research for the Bright Internet is characterized by two perspectives: first, the Bright Internet adopts a preventive security paradigm in contrast to the current self-centric defensive protective security paradigm. Second, the target of research is the development and deployment of the Bright Internet on a global scale, which requires the design of technologies and protocols, policies and legislation, and international collaboration and global governance. This research contrasts with behavioral research on individuals and organizations in terms of the protective security paradigm. This paper proposes validation research concerning the principles of the Bright Internet using prevention motivation theory and analogical social norm theory, and demonstrates the need for a holistic and prescriptive design for a global scale information infrastructure, encompassing the constructs of technologies, policies and global collaborations. An important design issue concerns the business model design, which is capable of promoting the propagation of the Bright Internet platform through applications such as Bright Cloud Extended Networks and Bright E-mail platforms. Our research creates opportunities for prescriptive experimental research, and the various design and behavioral studies of the Bright Internet open new horizons toward our common goal of a bright future.

Keywords: Bright Internet, Cybersecurity, Preventive Security, Origin Responsibility, Deliverer Responsibility, Identifiable Anonymity.

1 Introduction

The Internet has been primarily concerned with efficient massive transmission and wide propagation up to this point. At its beginning stages, the threat of anonymous users was not a primary concern because users were considered as mutually trustworthy researchers. However, the status of anonymous crimes and terror in cyberspace has become a serious issue and has indeed reached intolerable levels. Currently, users of Internet security systems must protect their own systems defensively, under the assumption that external attacks are uncontrollable. As such, the time has come for cyberspace to move from an anarchic age to an ethical age characterized by trust and responsibility in order to protect the safety of innocent global netizens.

In this paper, we propose the idea of the Bright Internet, which adopts the paradigm of preventive security by eliminating global sources of cybersecurity threats instead of merely defensively protecting users' own systems. For this purpose, assurances of traceability and the identifiability of malicious origins and deliverers are absolutely necessary. However, sacrificing legitimate rights to privacy and freedom of expression is also unacceptable, and adopting preventive security schemes may infringe on these rights. Thus, our challenging aim is to prescriptively design the Bright Internet so that these seemingly conflicting goals can be simultaneously achieved for innocent global netizens. Sharing the common vision, we define the Bright Internet as "the Internet that can preemptively reduce origins of cybersecurity threats by having the capability of identifying malicious origins and deliverers on a global scale, while maintaining the freedom of anonymous expression and a legitimate level of privacy protection for innocent netizens." Note that we distinguish innocent netizens from criminal ones because it is impossible to design a feasible solution without such a distinction.

The United Nations World Summit on the Information Society (WSIS) shared the same view with this definition, as declared in paragraphs 57 and 42 of the Tunis Agenda (WSIS, 2005) under the Chapter of Internet Governance:

> *57. "The security and stability of the Internet must be maintained*."
>
> *42. "… We affirm that measures undertaken to ensure Internet stability and security, to fight cybercrime and to counter spam, must protect and respect the provisions for privacy and freedom of expression as contained in the relevant parts of the Universal Declaration of Human Rights and the Geneva Declaration of Principles"*

However, there is no specific design theory yet developed that is capable of fulfilling these conflicting goals on a global scale; thus, little progress has been made in this direction. The problem can be solved neither by technology, nor policy alone. No single country can solve this problem, and there is also no commonly agreed-upon global design capable of solving this problem.

To cope with this complex problem collectively, the Council of the Association for Information Systems (AIS) adopted the Grand Vision Project for the ICT-enabled Bright Society (in short, the Bright ICT Initiative) in December 2014. The vision of the Bright Internet has focused, in particular, on the abovementioned issue, attracting the attention of numerous researchers in the information systems (IS) community. Lee (2015) sketched out the initial concept in an editorial article published in the *MIS Quarterly*. As a next step, this paper intends to formalize the goals and principles, and demonstrate the behavioral and design research of the Bright Internet so that follow-on studies can emerge.

The three goals of the Bright Internet are the following:

(1) Realize the preventive security infrastructure that can deter the motivation of cybercrime and terror originators;

(2) Maintain the freedom of anonymous expression for innocent netizens by distinguishing them from criminal ones; and

(3) Protect innocent netizens from the risk of privacy infringement that may be caused by adopting preventive security schemes.

To fulfill these seemingly conflicting goals, we propose five design principles based on prevention motivation theory and analogical social norm theory: principles of origin responsibility, deliverer responsibility, identifiable anonymity, global collaboration, and privacy protection, as shown in Figure 1. These five principles evolved from four principles initially proposed by Lee (2015). To equip the Bright Internet with the capacity to prevent state-led cyberattacks, we need to add a new set of principles, termed the Internet Peace Principles, as described in the second half of this special JAIS issue (Shin, Lee, & Kim, 2018).

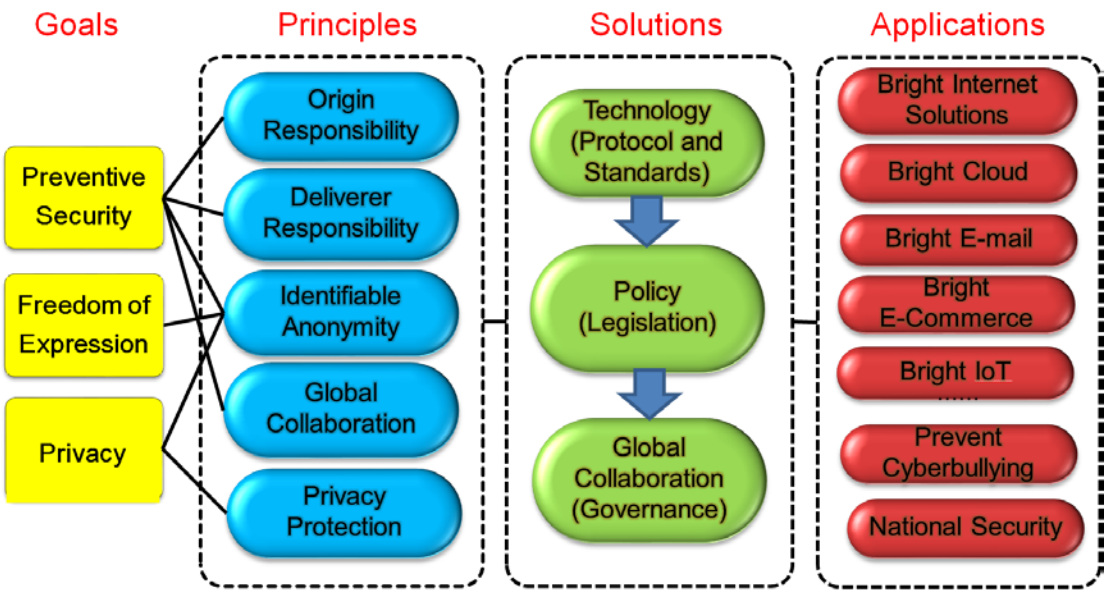


Figure 1. Goals, Principles, Solutions, and Applications for the Bright Internet

Research for the Bright Internet can be characterized according to two perspectives. First, the Bright Internet adopts a *preventive* security paradigm, in contrast to the current self-centric defensive *protective* security paradigm. We need to differentiate the preventative paradigm and demonstrate its benefit using its prototype and the empirical data collected from the test bed. Second, the target of our research is the development and deployment of the Bright Internet on a global scale, which will require the design of technologies and protocols (*technologies* in short), policies and legislation (*policies* in short), and international collaboration and global governance (*global collaboration* in short); this contrasts with behavioral research on individuals and organizations under the protective security paradigm.

In this paper, we propose validation research concerning the principles of the Bright Internet through prevention motivation and analogical social norms perspectives. An experimental study will be necessary to validate these principles. The comparative behaviors of different countries should also be studied in the context of current information system security theories. As such, this paper does not aim to complete the goal of our research, but rather seeks to open research opportunities and inspire contributions from our colleagues. This research contrasts with descriptive empirical studies in that the purpose of this research involves prescriptive research leading to the validation of principles for a safe next-generation Internet to come.

We also demonstrate the need for a holistic and prescriptive global-scale information infrastructure design, encompassing the scopes of technology, policy, and global collaboration. We propose a prescriptively specified technology requirement that can be propagated with consistency to the policy requirement and, in turn, the global collaboration requirement. We review this global scale design research from the design science perspective, although the factors to consider for its design differ significantly from the design of an organization information system (Hevner, March, Park, & Ram, 2004). Applications for business models may be designed after the Bright Internet platform is established. However, the opposite deployment approach may be adopted because a market-driven business model with killer applications can propagate the Bright Internet even without governmental regulation. In this paper, we offer some examples of business models in our discussion of the Bright Cloud Extended Networks and the Bright E-mail platform. The various application designs of the Bright Internet will eventually open a wide research horizon for business models development.

The remaining sections are organized as follows: Section 2 describes the typology of Bright Internet research by characterizing the preventive security paradigm, as contrasted with the protective security paradigm, and compares the design research of the global scale information infrastructure with the existing literature on individual and organizational behavioral research. Section 3 proposes the validation methods for the Bright Internet principles, and suggests the kind of experimental study that should be done as the next step of research. Section 4 designs the Bright Internet holistically, encompassing technologies, policies and global governance; we also

describe the market-driven business models here. Section 5 summarizes this paper, reviews the design of the Bright Internet from the perspective of design science, and proposes future research opportunities.

2 Characteristics of Bright Internet Research

The following reviews the progress of the Bright Internet Initiative, and contrasts Bright Internet research with the existing literature in the areas of information systems security and privacy.

2.1 Progress of the Bright Internet Initiative

The vision of the Bright Internet has been widely presented at many academic conferences, including the International Conference on Information Systems (ICIS 2015), Pacific Asia Conference on Information Systems (PACIS 2015), International Federation for Information Processing (IFIP), Information Systems Security Working Group (IFIP 2015), the AIS Special Interest Group (SIG) of Security and Privacy (SIGSEC 2015), IEEE/ACM International Conference on Utility and Cloud Computing (Lee, 2016b), and so forth. Along with active discussions on various panels and in workshops at AIS conferences, the research framework of Bright Information and Communications Technologies (ICT) and the Bright Internet are described by Lee (2015). The taxonomy of Bright ICT research has been elaborated, and the concept of Macro Information Society (McIS) research has been contrasted with organization-level Management Information Systems (MIS) research (Lee, 2016a). At ICIS in December 2015, the AIS and United Nations International Telecommunication Union (ITU) signed a memorandum of understanding on the joint pursuit of research and standardization of the Bright Internet framework as a potential platform for a trustworthy Internet.

The Bright Internet China Symposium was held at Xi'an Jiaotong University in June 2017, and the first AIS Bright Internet Global Summit was held as a pre-ICIS 2017 workshop in Seoul. The Journal of the Association for Information Systems (JAIS) is publishing a special issue on the Bright ICT Initiative (2018), where Shin et al. introduce the Internet Peace Principles.[1]

2.2 Preventive Security Paradigm versus Protective Security Paradigm

Current cybersecurity systems follow the *protective* security paradigm, which aims to protect their own systems from external attacks, under the assumption that the sources of attack are uncontrollable (Krebs, 2015). Typical solutions adopted for protective security are Anti-DDoS, firewalls, intrusion detection systems, anti-APT (advanced persistent threat), and threat management systems. Even if firewalls become higher and thicker, hackers will develop longer ladders to jump over them and more sophisticated drills to break through them. Even though intrusion detection systems (Rowland 2002) have been developed for known attacks, it is impossible to protect newly devised ones. APTs (Virvilis & Gritzails, 2013) spread their malware in several pieces across time, and thus make attacks more difficult to detect. Threat management systems aim to protect data leakage and intellectual property rights. The battle between the spear and the shield never ends, and there is no guarantee that the protection system is safe enough. As the Internet of things (IoT) becomes widely propagated, these attacks will even endanger human lives, and the damage will become more catastrophic. Small and medium enterprises can neither understand the entire spectrum of security problems and solutions, nor can they afford to invest in them. The Ponemon Institute reported that 80% of businesses cannot properly manage external cyberattacks, even though the solutions cost $3.5 million, on average, per year (Forrest, 2016). Shin et al. (2018) analyzed seven typical state-led cyberattacks cases from 11 factors of view.

In contrast, the Bright Internet aims to eliminate sources of external attack and adopts a proactive *preventive* security paradigm. This means that the origin servers will be evaluated by Bright Internet indices, and thus, servers will be motivated to filter outgoing malicious messages and deter the illegal access of criminal hackers using their servers. The origin servers will also be subject to a victim-driven reporting procedure. The two paradigms are contrasted in Figure 2. However, while origin servers will be motivated to take preventive measures, in response to either market-driven pressures or regulations imposed for societal benefit, it is nevertheless clear that the goal of the preventive paradigm cannot be fully achieved by individual organizations or countries alone. Therefore, due to the global nature of the Internet, the Bright Internet must be designed from a global perspective.

[1] A dedicated web page is available at www.brightinternet.org.

The necessity of preventive measures is also stressed in the Tunis Agenda (WSIS, 2005), paragraph 43, as follows: "We reiterate our commitments to the positive uses of the Internet and other ICTs and to *take appropriate actions and preventive measures, as determined by law, against abusive uses of ICTs* as mentioned under the Ethical Dimensions of the Information Society of the Geneva Declaration of Principles and Plan of Action."

We argue that it is necessary to balance the combination of protective and preventive security tools in order to minimize the total security risk and total security-related cost. For this purpose, it is essential that we pay more attention to preventive security research, such as Bright Internet research.

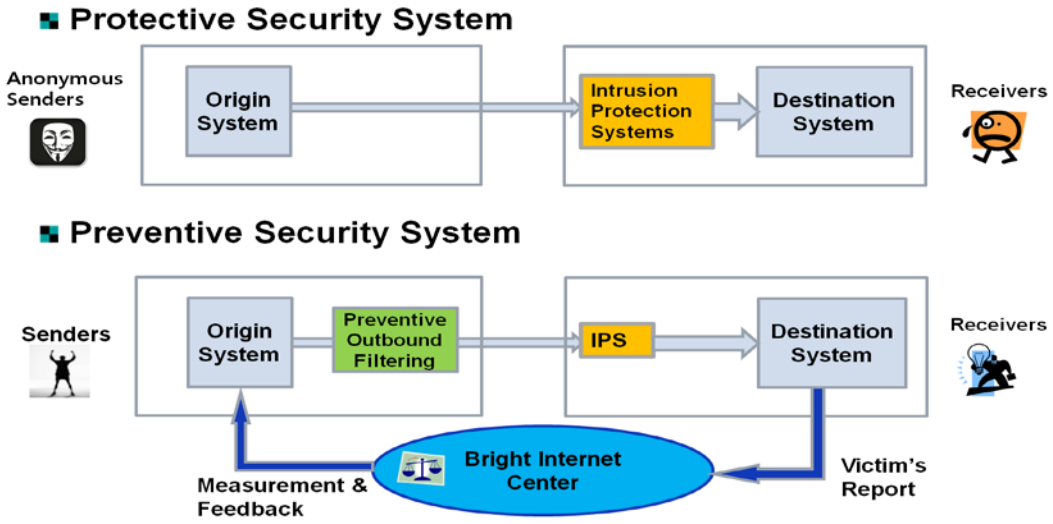


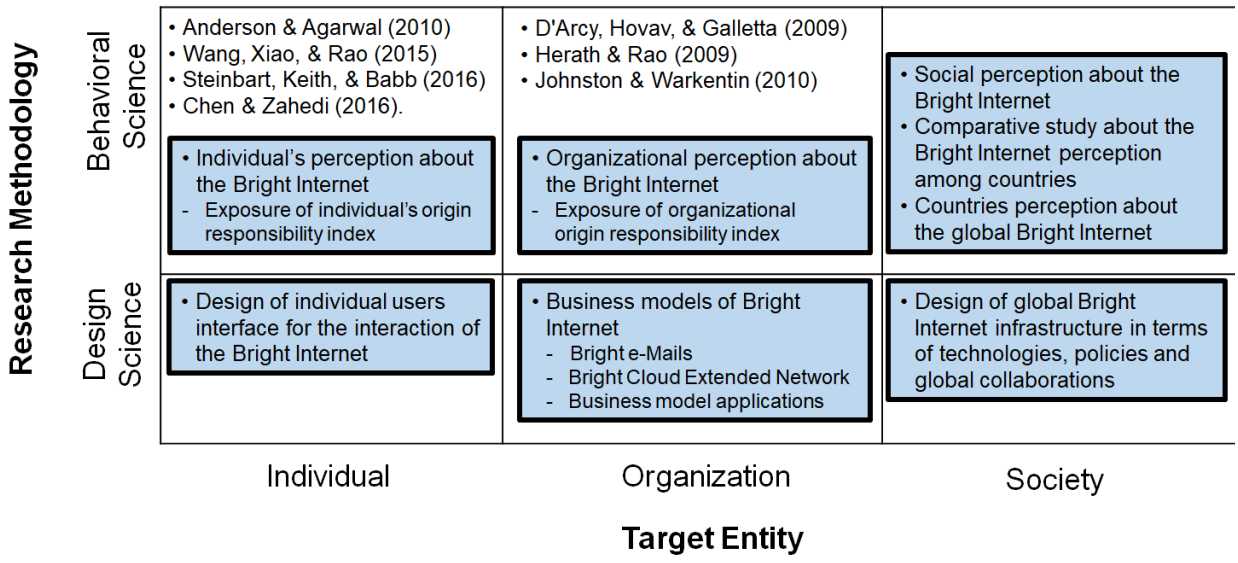
Figure 2. Protective Security Paradigm vs. Preventive Security Paradigm

2.3 Behavioral Research Concerning the Validity of the Bright Internet

Information security has been one of the fastest-growing research areas in the field of information systems. In fact, information systems journals have mainly focused on the behavioral research aspect, while engineering journals have focused on the design and technology aspects. The gap between the two communities has become wider, although integration between them is critical in solving real-world problems. To conceptualize the taxonomy of the information system security literature, in contrast with Bright Internet research, we classify selected articles published at major information systems journals into two dimensions, as in Figure 3. The horizontal axis denotes the target entity (individual, organization, or society), while the vertical axis indicates the research methodology (behavioral science or design science). Note that a broad range of theories from adjacent domains, such as economics, psychology, sociology, and even computer science, is applied to these studies.

It is worth highlighting that most previous studies assume that the sources of cyberattacks are uncontrollable and have investigated the issues in terms of protective security. Also, these studies rely on behavioral science research to determine the causes and effects of individual or organizational security. Most of these studies view security problems from the intraorganizational perspective, focusing on the attempts to protect against invasion or mitigate the misuse of information within the organization.

Thus far, no previous publications in the information systems field have investigated the design of a global scale Internet platform that aims to control the sources of external attacks. In this regard, Bright Internet research can be positioned as a global-scale social information system that requires a holistic design of the necessary technologies, policies, and global collaborations guided by the five principles. To understand netizens' perceptions about Bright Internet principles before the system is developed or deployed, we need a priori experimental research to justify its development. However, when the system becomes deployed in the future, a posteriori empirical research will be necessary to evaluate its performance in practice. Behavioral studies should be conducted at various levels of individuals, organizations, and countries. The discrepancy between different levels will generate useful policy implications. We review the perspectives of the existing information systems literature below.



Note: Typical examples of previous studies are presented in each category. Topics in the shaded box are potential research areas of the Bright Internet.

Figure 3. Position of Bright Internet Research

2.3.1 Behavioral Research of Information Security at the Individual Level

Individual behavioral studies have dealt with topics of behavioral security, protection motivation, and information security threat. With respect to these topics, protection motivation theory, coping theory, and information foraging theory have been investigated based on field studies, experiments and log data analyses. Understanding the context of the individual is important in research design, whether the individual is in the home, company, or society. For instance, Anderson and Agarwal (2010) studied the home computer user context and developed a model of the conscientious cybercitizen, suggesting that the security behaviors of home computer users are associated with cognitive, social, and psychological components. Wang, Xiao, and Rao (2015) highlighted two types of information security threats—unknown risk and dread risk—that yield a differential impact on information search behaviors in the context of university students' Internet use. Chen and Zahedi (2016) examined cultural differences in online security behaviors between the United States and China, and survey participants are recruited by university students in the United States and through online social networks in China. Steinbart, Keith, and Babb (2016) investigated individual behaviors affected by IT artifacts by creating a mobile application and a website to conduct a field experiment of 568 individual end users. Johnston and Warkentin (2010) conducted a survey experiment at a large university and concluded that fear appeals may have significant but differential impacts on the security-related behaviors of end users.

In contrast, at its early stage of design, Bright Internet research requires *experimental* studies to assess individuals' perceptions about Bright Internet principles. Such studies will help to clarify the prescriptive requirements of netizens for the next-generation Internet. If individuals are reluctant to accept preventive security principles, but feel that such principles are necessary for society, voluntary acceptance will likely be difficult, and these principles will need to be regulated or otherwise motivated. Creating market-driven business models, such as "trustworthiness as an asset" (e.g., when individuals voluntarily authenticate themselves in order to use credit cards), are important research opportunities that could assist in motivating individuals to voluntarily participate in the new principles of the Bright Internet, even without regulation. Studies of individual perceptions can also extend to the national cybersecurity perspective. A comparative international study regarding the priority of the five principles would be interesting and insightful for understanding differences between countries and figuring out what principles could be adopted for a global common platform. A group of scholars in South Korea, the USA, China, and other countries is currently working on this issue.

2.3.2 Behavioral Research of Information Security at the Organizational Context

Organizational behavioral studies have dealt with topics of security management, security policy compliance, behavioral security, organizational information security policy, information disclosure, software vulnerability, and information systems security. These papers have examined general deterrence theory, protection motivation theory, principle agent theory, social control theory, and neutralization theory based on field studies, database analyses, and framework development. Willison and Warkentin (2013) highlighted that while previous studies have primarily focused on individuals' security compliance decisions, it is necessary to extend our view toward the interplay between the thought processes of offenders (that may precede the violation) and the organizational context.

There is a stream of studies related to internal information security policy/technology and human-related issues. For instance, in order to understand delinquent behavior, Herath and Rao (2009b) proposed a principal-agent paradigm by emphasizing the proper level of sanctions. Bulgurcu, Cavusoglu, and Benbasat (2010) identified the importance of factors such as attitude, normative beliefs, awareness, and self-efficacy that force employees to comply with information security policies. Similarly, Herath and Rao (2009a) and D'Arcy, Hovav, and Galletta (2009) used general deterrence theory to explain employees' compliance intentions. Their findings suggest that organizational commitment, social influence, and user awareness of security countermeasures are important factors contributing to internal security-related rules or reducing IS misuse. Consistent with previous work, Hsu, Shih, Hung, and Lowry (2015) argued for the significance of organizational extra-role behaviors (security behaviors that are not specified in information security policies). Their findings also emphasized that social control (e.g., employees' commitment, attachment, and beliefs) may play a pivotal role in enhancing both in- and extra-role security behaviors. Mitra and Ransbotham (2015) further examined how the degree of disclosure on software vulnerability affects the diffusion of attacks. Their findings suggest that full disclosure of vulnerability may lead to a faster diffusion of attacks and a higher risk of the first attack than a situation of limited disclosure.

Prescriptive experimental studies on an organization's behavior or an individual's behavior in the organization while participating in Bright Internet services and business could generate interesting research topics. These studies would be able to demonstrate new business models, which could create a new horizon of trustful services who adopt the Bright Internet platform. For example, the effects of disclosing a company's origin responsibility index would be an important research topic that would change the behavior of preventive security activities. If individuals in a company were reluctant to accept preventive security principles but felt that it was necessary for the company, such a principle could be enforced by a company-level policy.

2.3.3 Privacy Research

According to privacy research in the information systems community, many agree that the privacy issue is a multidisciplinary diverse concept (Oetzel & Spiekermann, 2014). Thus, a broad range of studies on privacy deals with various aspects from different angles and points of view. Bélanger and Crossler (2011) have nicely and thoroughly reviewed the literature regarding privacy in the field of information systems.[2] They concluded that most privacy studies in the information systems domain have been conducted at the individual level of analysis.

Although these studies are important in understanding privacy concerns and the attitudes of users under various practices and circumstances, they are not sufficient in providing actionable solutions. In this regard, Bélanger and Crossler (2011) highlighted the following: "Information systems research should focus more on design and action with an emphasis on building actual implantable tools to protect information privacy." They also argued that it is necessary to conduct privacy-related studies at the societal level rather than at individual, group, or organizational levels. Similarly, Pavlou (2011) suggested that future studies on privacy in the information systems domain should address the design science perspective, which aims to build the tools and technologies regarding various aspects of information privacy. He also emphasized that future studies should examine users' incentives from the point of view of the economics of information privacy.

It seems that the fifth principle of privacy protection in Bright Internet research is very much in line with this sentiment. Designing a preventive security scheme without infringing on privacy is a very important and challenging issue. If we regard all netizens homogeneously, then security and privacy have a nondominated relationship with each other, which means that it is necessary to sacrifice one element in

[2] For the sake of brevity, we do not provide a comprehensive literature review regarding information. Instead, we focus on the future direction of studies suggested by review papers (Bélanger & Crossler, 2011; Pavlou, 2011).

order to realize the other. However, if we distinguish innocent netizens from criminal ones, it will be possible to design a preventive security system against criminal netizens while protecting the privacy of innocent netizens. This is a goal that Bright Internet research must fulfill.

3 Validation of Bright Internet Principles

Justifying the validity of the goals and design principles of the Bright Internet requires an appropriate research framework. For this purpose, we propose two approaches: *prevention motivation theory* and *analogical social norm theory*. We hypothesize these theories so that follow-on researchers can test them with data. Future research on the theoretical implications of the principles and the identification of their antecedents are open research questions. Such research would potentially evaluate the pros and cons of the current principles, add new principles, or replace certain principles with more effective principles.

3.1 Validation with Reference Theories

3.1.1 Prevention Motivation Theory

We argue that the design goals of the Bright Internet should be justified by the seriousness of prevention motivation. The prevention motivation has been widely implemented in the field of preventive medicine. We term this concept prevention motivation theory. This theory is similar to protection motivation theory (Rogers, 1975) in a social context, which maintains that people take protective actions in relation to their fear of a severe threat and the high probability of its occurrence. Prevention motivation theory, on the other hand, also considers additional factors—the possibility of self-protection failure, the possibility of preventively eliminating the origins of cyberattacks, and the cost-effectiveness gap between prevention and protection. In other words, if Internet users are increasingly fearful of cybersecurity threats with a high probability due to the possibility of protection failures, it can be argued that designing the proper goals and principles to prevent potential sources of threat is of benefit to society. Despite the importance of the preventive approach, this aspect has been largely neglected in previous studies.

In order to measure the individual's prevention motivation using the Bright Internet, Cho and Lee (2016) conducted a preliminary survey on the security risk perceptions of approximately 1,500 netizens in Korea. Based on the classification of cybercrime statistics from the FBI and the ITU, they selected the seven most commonly occurring security risk factors on the Internet for this survey—cyberterror, financial fraud, privacy leakage, flaming/trolls, online censorship, spam emails, and child-harmful content. The survey results are summarized in Table 1, indicating that most survey respondents believed the current Internet space to be either "very vulnerable" or "vulnerable" to each risk factor. That is, it is necessary to adopt new principles of the Bright Internet to prevent or reduce prominent sources of risk on the Internet. A group of researchers is currently working on the theoretical development and a comparative international study on this topic. This global research partnership offers an open opportunity for scholars in relevant fields of study.

Table 1. Summary Statistics of Vulnerability Perceptions toward the Current Internet

	Cyberterror	Financial Fraud	Privacy Leakage	Flaming and Trolls	Online Censorship	Spam Emails	Child-harmful Content
Mean	2.079	2.163	1.707	1.725	2.083	1.619	1.748
Std. Dev.	0.803	0.869	0.814	0.863	0.852	0.798	0.859
Note: degree of vulnerability perception (1: very vulnerable; 5: very protective)							

3.1.2 Analogical Social Norm Theory

To justify the validity of design principles that have not yet been physically implemented, it is reasonable to infer implicit social norms about the principles from similar existing conventions. We call the justification approach based on analogical references the analogical social norm theory. In the case of the Bright Internet, inquiring about social norms regarding a nonexisting complex artifact is very difficult, and thus, ordinary respondents cannot precisely understand the meaning of these principles. Therefore, as Chaturvedi, Dolk, and Drnevich (2011) have argued, such inquiries may be guided by analogical reference cases. Identifying the suitable analogical social norms can serve as the first step of persuasion. Elster (1989) studied the effect of self-interest in building social norms, and Coleman (1990) found that social sanctions enforce social

norms. In this paper, we demonstrate analogical cases about the Bright Internet principles which we have identified so far. Further study in terms of legal perspectives will reveal additional social norms. For instance, ten statements of the Internet Peace Principles were derived from two analogical conventions from non-IT domains, including the Treaty on the Non-Proliferation of Nuclear Weapons, in addition to four extendable traditional conventions (Shin et al., 2018).

3.2 Validation of Principles

We now turn to defining the five design principles, and justifying them individually based on prevention motivation and analogical social norms (social norms, in short).

3.2.1 Principle of Origin Responsibility

Definition: *The principle of origin responsibility means that the offensive originators of malicious codes and illegal hacking should be responsible for the consequences of their malicious behaviors.*

Under the principle of origin responsibility, the ethics of computer users should be extended to the level of avoiding attacking others in order to socially protect one another. To prevent cybercrimes and cyberterror, the responsible origin IP address and real names should be traceable if the cyberattack is detected and a legitimate search warrant is issued. However, criminals spoof their origin IPs and hide their real names. That is why the complementary principles of deliverer responsibility and identifiable anonymity are necessary.

Prevention Motivation

Billions of spam emails, possibly with hidden malicious codes, are sent globally every day, occupying about 54.2% of all email traffic (Shcherbakova, Vergelis, & Demidova, 2015). Therefore, it is impossible to protect individual recipients from such attacks by through protective measures alone without eliminating the originators of malicious emissions. According to deterrence theory, tracing the origins of responsibility is the most effective scheme for the prevention of cyberattacks (Herath & Rao, 2009a; Nagin, 2013). As a result, it is necessary to identify the originators and make them take responsibility for the consequences they have caused. To realize this principle, it is necessary to design the Internet protocol so that it can fundamentally prevent spoofing, possibly by using IPv6.

Social Norms

This principle is almost a natural law in human society; however, it has not played out that way in anonymous cyberspace. In the current protective security paradigm of the Internet, anonymous attackers from detoured countries can hide their origins, and victims at the destination end up taking the responsibility, which contradicts the ethical standards of civilized society.

The treatment of electronic hardware waste serves as an interesting reference practice. The European Union (EU) Directive of Waste Electronic and Electric Equipment (WEEE) (Rossem, 2008) adopted the principle of individual producer responsibility for the safe disposal of electronic waste (Lee, 2015). Through adopting this principle, third-party waste collectors, such as the Europe Recycle Platform in Europe, collected 2 million tons of electronic waste across 17 countries in 2014 (ERP, 2014). Introducing non-monopolistic business practices for waste collection led to a decrease in collection costs from 70 euro cents per kilogram in 2005 to 7.5 euro cents in 2007 (Lee & Shao, 2009).

This example provides analogical insight into how to best control the spread of malicious software codes through adopting the principle of origin responsibility, by illustrating how this principle could potentially reduce the generation of malcodes and reduce operational costs through competition. As such, adopting this principle could create a quantum leap in terms of cybersecurity ethics and new business models.

Chain of Origin Responsibility

However, it is not always clear who the responsible origin is. There are many layers of origins, including the individual, server, company, and country (Lee, 2015). The concept of origin will require further classification in terms of each role—including the maker, owner, user (e.g., hacker or passenger), and driver (e.g., software agent or autonomous car)—as the application expands to the IoT domain. The legal responsibility of roles must be defined, and the responsible role performer should be traceable if a crime is detected.

As a first step of research, let us assume a simple case of a hacker accessing an origin IP and conducting malicious cyberattacks. The elementary base of origin is the individual who accesses a server, sends malicious messages, and/or hacks other sites; and the responsibility of an individual's misconduct should be borne by the originating individual. These kinds of offensive originators can be identified by an innocent server manager who can easily verify and control them. However, if the individual is not identifiable due to the negligence or malicious intention of the server manager, the server manager, or the company at a higher level of the chain, should take full or partial responsibility for the individual's misconduct. Therefore, a regulation should be established to implement a chain of responsibility in order to prevent

intentional evasion by a company. As such, a chain of reporting responsibility is necessary, as described below.

Individual-layer origin: If an individual user of a server acts maliciously through a server, the server manager should be able to trace the individual in order to stop the behavior and possibly request compensation for the behavior and/or consequences. This concerns the individual layer of the origin. Thus, it is necessary to motivate server managers to take such actions. Chained responsibility will motivate server managers to prevent the unidentified malicious use of their servers and encourage the use of a system that traces malicious individuals who repetitively misuse their servers. Public Internet service providers, such as cloud service providers, game rooms, and Wi-Fi services, should be alerted so that their servers do not become a backdoor for criminal activity. Recently, the European Union's highest court decided to advise open Wi-Fi hotspot owners to require users to input passwords and to be capable of confirming their identities (Orlowski, 2016). There is a societal tradeoff between free access and security.

Server-layer origin: If a company has multiple servers, each server manager can operate as the center of responsibility from the company's point of view. If the server managers themselves have malicious intentions, they will not trace or report the individual origin's malicious behaviors in which they are involved. This means that the company who owns the server should monitor the behavior of the server managers, or risk being held responsible for their negligence. This chain of responsibility will motivate companies to monitor and prevent their servers from being misused.

Company-layer origin: Companies comprise the next level of responsibility for those who use their computing resources. These companies should monitor whether their resources are being misused to attack others. However, if a company itself is a malicious organization, the government is the authority who should monitor the malicious behaviors of such companies. If the company does not fulfill its reporting responsibility, even though there is clear evidence provided by the victims of their attacks, the company itself should be regarded as a malicious organization. Such malicious companies should be monitored by an authorized government agency. This is analogous to a corporation's tax reporting responsibility regarding their employees' taxes.

Country-layer origin: The country is the highest level of responsibility. However, if a country itself is the origin of cyberterrorism, the government will not trace or report the responsible company or individual origin (Shin et al., 2018). In this case, the country should be monitored by a global governance body and should be held responsible for its malicious behaviors. The global governance body should enforce the Internet Peace Principles, measure damages, and determine appropriate compensation and sanctions. The chain of origin responsibility demonstrates the need for protocols, technologies, national regulations, and international agreements.

3.2.2 Principle of Deliverer Responsibility

Definition: *The principle of deliverer responsibility means that compromised computers or Internet service providers who are involved in the delivery process of cyberattacks, even unintentionally, should cooperate to prevent delivering identifiable harms to the users at the destination.*

Under the principle of deliverer responsibility, the ethics of computer users should extend to the level of not being abused to attack others so as to socially protect one another.

Prevention Motivation

Research suggests that 90% of spam emails are sent from compromised computers (Lawson, 2012), and typical DDoS attacks utilize millions of compromised computers. This phenomenon demonstrates that it is essential to make an effort to protect all computers so that they will not be compromised as deliverers of malicious codes.[3] A security software provider could potentially extend the function of their solution to include the principle of deliverer responsibility.

The second type of deliverer is the Internet service provider (ISP), which carries out most of the last-mile delivery. In Korea, the top 10 ISPs delivered 86% of spam mails. These spam emails may include phishing, scams, and malware. However, ISPs do not filter these spam emails because they prefer to maintain network neutrality and do not want to take responsibility for harmful delivery. Nevertheless, ISPs should cooperate with the prevention of malicious code dissemination. As such, the principle of deliverer responsibility is necessary because the principle of origin responsibility alone cannot completely eliminate malicious attacks.

Social Norms Concerning Comprised Computers as Deliverers

An analogy for deliverer responsibility is the misuse of stolen guns, whether or not the owner recognizes them as stolen. It is controversial how much legal responsibility should be accepted for carelessness

[3] For more information, visit the website www.digitalattackmap.com to see daily DDOS attacks worldwide.

or negligence in preventing the malicious misuse of risk-creating items. Nevertheless, most netizens agree that we should protect one another. As a result, a security software solution provider, possibly in cooperation with the OS provider, could install and update preventive tools with appropriate business models and/or regulations.

Social Norms Concerning Internet Service Providers as Deliverers

The Council of the European Convention on Cybercrime stipulates that ISPs in Europe are responsible for surveillance. China also allows surveillance. The USA and Korea have not allowed surveillance in the past; however, recently their congresses have passed antiterrorism acts to detect plots and prevent serious acts of terrorism. Therefore, it seems that it would be reasonable to empower ISPs to filter identifiable malicious messages. Whether ISPs or security authorities should conduct such surveillance is a design issue.

Analogical cases can be found in the inspection areas at airports and monitoring by CCTV. Therefore, this practice is analogous to the ISP-based surveillance in cyberspace. Records of innocent citizens on CCTV should not be traced unless the records are associated with certain incidents. Similarly, ISP-based surveillance should make sure that it does not infringe on the privacy of innocent netizens.

3.2.3 Principle of Identifiable Anonymity

Definition: *The principle of identifiable anonymity means that the real name or equivalent identity of criminal origin should be identifiable in nearly real time in the context of a valid search warrant, while the voluntary anonymity of innocent netizens should be preserved.*

This principle seeks to fulfill two seemingly conflicting goals of identifiability: the need to both identify criminals and to preserve the anonymity of innocent netizens. Thus, we must design an appropriate method to simultaneously meet these two goals. There is a difference between identifiability and authentication: A narrow sense of identification refers to confirming a real name (in contrast to a pseudonym), while authentication refers to confirming that the person is truly the same as the digital identity. A broader sense of identification may, perhaps, include the authentication process, but in this study, we adopt the narrow sense to distinguish between the two endeavors.

Prevention Motivation

Even though the IP address of the attack origin may be traced, criminal originators will not use their real names or the equivalent. This is why the real names of anonymous users should be identifiable if criminal behavior is detected and a valid search warrant is issued. Evidence of malicious behaviors often evaporates within a week. Blue Coat Systems researchers reported in their "One-Day Wonders" security report that 71% of host names disappear within less than 24 hours (Horst, 2014), and criminal web pages last, on average, about a week in cloud service sites (Kolthof, 2015). These observations indicate that the real-time assurances of large-scale traceability and identifiability against criminal actions are essential.

However, human rights activists insist that online anonymity is necessary to protect freedom of expression. A few careful designs can fulfill both goals. For this purpose, the Bright Internet does not have to completely replace the current Internet platform, just like credit cards do not completely replace cash. Both may coexist, and the Bright Internet is an optional platform for those who want a safer platform for certain applications with trustworthy people. One person may hold accounts on both platforms; thus the Bright Internet will not destroy the possibility of online anonymity, and the concerns of human rights activists can be taken into consideration within the concept of identifiable anonymity.

Social Norms

It is our premise that the intention of crime can be most effectively deterred if the offender is identifiable. An extreme case of identifiable anonymity is voluntary real-name registration, as is already done to register credit cards and online banking accounts. Unless a cardholder commits a financial crime, the client's private records should be protected and should not be illegally disclosed. The business benefit of real-name registration can be seen in a case involving online auction markets. In 2002, auction.co.kr in Korea (the current eBay Korea) required real names to eliminate illegal cash-back transactions using credit cards. They were shocked by the sharp decline in the total number of registered clients, but it was interesting to observe that they achieved even higher successful bids, and eventually higher total revenues (Lee, 2002). This example demonstrates that the adequate demarketing of fake clients by adopting a real-name system enhances the level of trust and also reduces the unfruitful waste of resources caused by malicious users.

3.2.4 Principle of Global Collaboration

Definition: *The principle of global collaboration means that in order to implement the principles of the Bright Internet on a global scale across borders, it is essential that Internet user countries collaborate globally in terms of communication, cooperation, execution, and reporting.*

Prevention Motivation

Malicious attackers tend to detour their routes through third countries to obscure their origins and make coordination between countries more complex. Thus, an international agreement between the relevant countries to ensure cross-border traceability and identifiability is essential. Each country may have different rules of regulation for their national security. Thus, governments should work together to establish commonly accepted rules of cooperation; such agreements should be global in order to prevent the emergence of a cybercrime haven territory.

Social Norms

There are a few international organizations that play the role of global Internet governance, such as the UN Group of Governmental Experts (GGE), Internet Governance Forum (IGF), UN International Telecommunication Union (ITU), Internet Engineering Task Force (IETF), and Internet Corporation for Assigned Names and Numbers (ICANN), as well as academic organizations, such as AIS, Institute of Electrical and Electronics Engineers (IEEE), Association for Computing Machinery (ACM), and International Federation for Information Processing (IFIP). However, their activities are not effectively coordinated with each other toward global governance in terms of a safe next generation of the Internet. That is why forums such as the Bright Internet Global Summit and Bright Internet Global Organization (BIGO) are needed; they give multistakeholders the opportunity to collaborate on technical, policy, and global issues, and seek agreement on a common vision and principles. When the BIGO reaches consensus among member countries, BIGO will be able to cooperate with authorized governments and international organizations, such as the United Nations.

3.2.5 Principle of Privacy Protection

Definition: *The principle of privacy protection here means that the Bright Internet system should be technically and legally designed in consideration of protecting privacy, which may be threatened by adopting preventive security-related principles.*

The general concept of privacy protection is very broad, but in this research, we focus only on the risks that may be introduced by adopting the four security-related principles of the Bright Internet. The principle of identifiable anonymity already seeks to protect the privacy of innocent netizens by limiting the inquiry of real names only if digital search warrants are issued.

Preventive Motivation

Surveillance at the origin servers and deliverers may monitor and collect private information, which may increase the risk of privacy infringement. However, directly requiring a real name at a registration site may increase the risk of information leakages. Global collaborations may further extend the risk of privacy information leakages among countries. Therefore, it is necessary to prevent potential risks that may be caused by the implementation of these principles, both technically and legally.

Social Norms

As mentioned earlier, paragraph 42 of the Tunis Agenda states that privacy should be protected in balance with cybersecurity. We explicitly adopt this principle here, because unless the technical and legal protections of privacy are ensured, many netizens will be reluctant to accept preventive security principles, even if they agree with the necessity of preventive security. Designers of the preventive security scheme should take privacy protection into account, in order to avoid, or at least minimize, such a risk.

4 Design of the Bright Internet

4.1 Design Theory of Bright Internet Research

Designing the Bright Internet based on the above-mentioned principles necessitates a holistic design of a global scale Internet infrastructure and a global governance structure. So far, there has been design science research at the firm level (e.g., Adomavicius, Bockstedt, Gupta, & Kauffman, 2008), but no previous publications in the information systems field have investigated the design of a new Internet platform capable of preventing the sources of security threat. In this sense, Bright Internet research can be regarded as a global information system infrastructure creating the foundation for all future business and social information systems.

For this purpose, Figure 4 proposes the framework of the *design activities of global societal information infrastructure*, which our design of the Bright Internet 1.0 in this section instantiates, and which contrasts with the *design activities of organizational information systems* (Hevner et al., 2004). To justify the fit with the design science framework, Bright Internet design activity is reviewed in Section 5 from the perspective of seven guidelines (Hevner et al., 2004): the artifact, relevance, design evaluation, research contribution, research rigor, design as a search process, and communication of research.

Since we cannot demonstrate design principles with a developed prototype of a complex system in its beginning stages, our design principles can be regarded as a top-level prescriptive design specification (Kuecheler & Vaishnavi, 2012). The constructs and variables (Arnott & Pervan, 2012) can be derived from these design principles. The complex global

information infrastructure should simultaneously encompass the domains of technologies, national policies, and global collaboration, because these variables are tightly interrelated with one another.

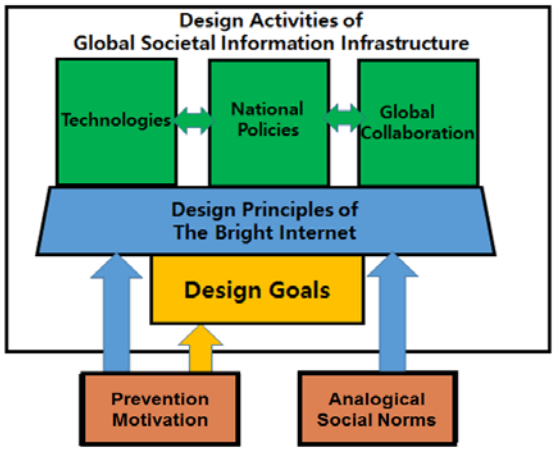


Figure 4. Design Activities for the Global Societal Information Infrastructure

4.2 Principles-Driven Holistic Design

Based on the five principles of the Bright Internet proposed above, we prescriptively design three constructs (technologies, policies, and global collaboration) and design variables as follows.

4.2.1 Prescriptive Design Process

Step 1 (technology design): For each principle, define the necessary technologies by designing the protocols and systems.

> Step 1a: Identify what new technological research is necessary to meet the technological requirement.

Step 2 (policy design): Define the national policies that are consistent with the technological design.

> Step 2a: Identify what laws and regulations should be established and/or amended to realize the new policies.

Step 3 (global collaboration design): Define the global collaborations that are necessary among countries that are compatible with the national laws and technologies.

> Step 3a: Identify what new global agreements and governance are necessary.

The beauty of the prescriptive design is that is allows us to build an experimental test bed for technology, policy and global collaboration, which provides the starting point of discussion. It will be necessary to gather feedback and learn from the design of a complex sociotechnical system. Recall the Simonian artifice mode of inquiry in design science, which requires constructive interactions among people, artifacts, and the environment (Baskerville, Kaul, & Storey, 2015). As such, if an agreement about national policy and/or global collaboration cannot be reached, at a certain point we will need to propagate the constraints back to the technical design and keep consistency within it. As such, understanding the interaction effect between policy and technology is important for a consistent design. To ensure consistency between design variables, it may be necessary to employ the notion of constraint satisfaction problems (Lee & Kwon, 1995).

The importance of prescriptive knowledge in design science research is recognized as Singerian progress by Baskerville et al. (2015). More than one design can achieve the principles, and designs should thus compete with each other, with more innovative designs replacing older ones. Considering the interactions among the design variables, the design process can be iterative. In this paper, we demonstrate the design of Bright Internet 1.0 as the first outcome of our own research. The target of this research is an invention of a new system, in contrast with the improvements and exaptations presented in other studies (Gregor & Hevner, 2013), according to the science of the artificial perspective (Simon, 1996).

4.2.2 Business Model Driven Deployment Strategy

The holistic design is comprehensive, but full-fledged development and deployment will take a long time. Thus, a middle-out deployment approach with killer applications will be necessary. According to this approach, not all principles must necessarily be adopted at once, depending on the goals of the applications. For instance, a cloud service provider could the Bright Internet platform, building Bright Cloud Services. Multiple Bright Clouds could be connected to each other via a virtual private network expanding to the Bright Cloud Extended Network. The origins of tenets in the Bright Cloud Extended Network would be identifiable to each other and thus could trust each other. Thus, this idea could be a new business model motivating cloud service providers to upgrade their services with a high level of trust. As additional cloud service providers join the Bright Cloud Extended Network, the Bright Internet could be propagated accordingly.

Another appealing application would be Bright E-mail services. Victims of malicious spam mails could report them to the Bright Internet Center, which would work with lawyers to file collective compensation lawsuits against the malicious origins. The Bright Internet Center would also globally publicize the bad neighbors, which would encourage origin servers to perform origin responsibility to protect their own businesses. The collected compensation could be paid back to reporting victims, and this—in addition to the

increased collective security—would incentivize them to report. Bright E-commerce, Bright Auctions, Bright Shared Economies, Bright Fintech and Bright IoT are all potential applications of the Bright Internet platform, as depicted in the application layer of Figure 1. Such applications will increase the popularity of the Bright Internet, and motivate businesses to move to the Bright Internet platform.

4.3 Design of the Bright Internet 1.0

We demonstrate the design of the Bright Internet 1.0 in terms of the technologies, policies and global collaborations, as depicted in Figure 5. Note the interrelationship among them, as we describe them individually below.

4.4 Design of Technologies

The design variables of different technologies are classified by the principles denoted by *TO* (technologies for origin responsibility), *TD* (technologies for deliverer responsibilities), *TI* (technologies for identifiable anonymity), *TG* (technologies for global collaboration), and *TP* (technologies for privacy protection).

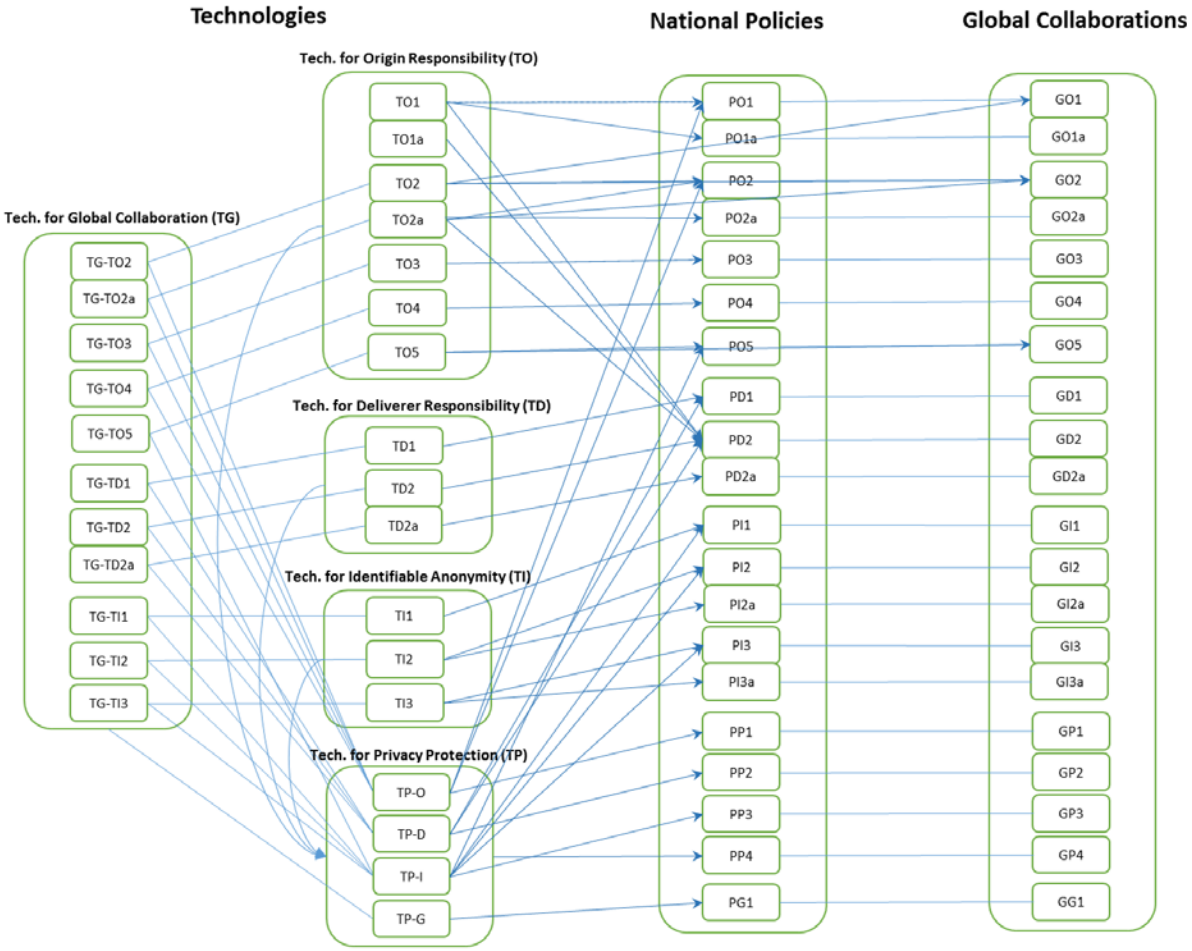


Figure 5. Design Variables and their Relationships

4.4.1 Technologies for Origin Responsibility (*TO*)

Technologies for origin responsibility are necessary for the prevention of outgoing malicious codes (*TO1*), identification of parsimonious surveilling targets (*TO1a*), record-keeping of repeatable risk sources (*TO2*), evaluation of the impact of attacks (*TO2a*), victim-initiated reporting procedures (*TO3*), overall architecture and process for the management of origin responsibility (*TO4*), and traceability of the origin IP address (*TO5*).

TO1: Architecture of an origin-based preventive system

TO1a: Identification the parsimonious target objects of origin server's surveillance

TO2: Sharing mechanism of the list of repeatable risk sources

TO2a: Development of the evaluation model of attacks and attackers

TO3: Victim-initiated reporting procedure

TO4: Architecture, management, and protocol of origin responsibility

TO5: Technology for origin IP address traceability

For screening in *TO1*, the antivirus vaccine software and other intrusion detection systems may be applied in reverse. The victim-initiated reporting procedure will create an origin-destination relationship matrix database of malicious codes, which can motivate originators to reduce the generation of malicious codes. Tracing technology for *TO5* may not be possible on a simple TCP/IPv4. Therefore, we need to upgrade the Internet protocol to the improved IPv6 in order to prevent the fabrication of the original IP address (Bi, 2016).

4.4.2 Technologies for Deliverer Responsibility (*TD*)

Technologies for deliverer responsibility will be used to prevent zombie computer attacks and screen malicious codes during the intermediator's routing process. These technologies are necessary to filter the malcodes that were not screened out by origin servers. Since it is not easy for ordinary users to take preventive actions to avoid being compromised, the security solution and/or operating system software makers should take preventive measures on behalf of PC or smartphone owners (for *TD1*). Likewise, a security solution provider may take preventive measures for the network (for *TD2 and TD2a*).

TD1: Design of the preventive system for potential zombie computers

TD2: Design of the intermediator-based preventive surveillance system

TD2a: Identification of the parsimonious target objects of the intermediator's surveillance

4.4.3 Technologies for Identifiable Anonymity (*TI*)

Technologies necessary for identifiable anonymity include the architecture of identifiable anonymity, methods of real-name identification, and digital search warrant management systems.

TI1: Development of the architecture for identifiable anonymity

TI2: Adoption of appropriate methods for direct and indirect real-name identification

TI3: Development of digital search warrant management systems

The architecture of *TI1* will adopt two layers of identification: The *freedom of expression layer with pseudonyms* and the *security layer with real names*, as in Figure 6.

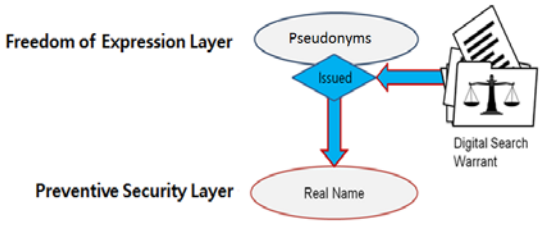


Figure 6. Freedom of Expression Layer and Preventive Security Layer

The methods for real-name identification for *TI2* can be classified as *direct identification* and *indirect identification*. A suitable method may be selected, depending on the company's strategy.

a. *Pure real-name identification:* If real names are already adopted, such as in banking systems, they can be shared for the Bright Internet applications.

b. *Direct identification:* Pseudonyms and real names are collected directly and stored simultaneously.

   1. *Parallel identification:* When a real name can be confirmed at the registration site, both the pseudonym and real name can be collected simultaneously. Some offline business partners, such as banks and telecom companies, can authenticate and register both names together.

   2. *Certificate extended identification:* When there are certified real names already registered for a certain application, such as a certification authority, credit card or bank account, the pseudonym may be linked to these certified sources, which can be used a source of real names.

c. *Indirect identification:* If the clients of an organization, such as Google Gmail, fear the leakage of stored real names, the real name can be inferred from multiple indirect data, rather than stored directly. For instance, Airbnb does not require a certificate at remote sites, but requests multidimensional information, such as e-mail address, phone number, SNS site, work address, and personal information, which can be of help for the inference of real names. However, the indirect method may not definitely guarantee the identifiability of real names. In case a service

organization fails to identify the real name, it is debatable how much the organization should take responsibility for the evaded damages.

The digital search warrant management system in *TI3* requires the function of application, issuance, execution, and reporting procedures. To handle thousands of cases every day consistently and efficiently, a rule-based supporting tool may be necessary.

4.4.4 Technologies for Global Collaboration (TG)

When the technologies developed for the three security-related principles are applied across national borders, factors that occur between countries become important. When two countries have different policies, they must first establish commonly agreeable collaboration that is mutually beneficial in fighting cybercrime. The global collaboration model applied to multiple countries for each technology, is denoted as *TG*, followed by *O*, *D*, and *I*, depending on the basic technologies in the *TO*, *TD* and *TI* categories.

TG-O2: Mechanism of the list of repeatable risk sources on a global scale

TG-O2a: Global evaluation model of attacks and attackers

TG-O3: Global victim-initiated reporting procedure

TG-O4: Global architecture and protocol standard for Bright Internet principles

TG-O5: Technology for origin IP address traceability in the global context

TG-D1: Global preventive system for potential zombie computers

TG-D2: Intermediator-based preventive surveillance system across borders

TG-D2a: Identification of the parsimonious target objects of the intermediator's surveillance across borders

TG-11: Architecture for identifiable anonymity in the global context

TG-I2: Methods for direct and indirect real-name identification in the global context

TG-I3: Digital search warrant management systems across borders

4.4.5 Technologies for Privacy Protection (TP)

Privacy protection technologies aim to audit the Bright Internet system to insure that there is no illegitimate infringement of innocent netizens' privacy by the surveilling agents. The design seeks to maintain privacy by empowering a trustworthy technical and legal audit capacity, while maintaining preventive security. The auditing process should cover all of the following principles.

TP-O: Privacy protection audit against origin responsibility

Minimize the number of surveillance objects by utilizing data analysis techniques effectively.

TP-D: Privacy protection audit against deliverer responsibility

Audit the risk of surveilled information being used maliciously.

TP-I: Privacy protection audit against identifiable anonymity

Audit the risk of real-name information being leaked.

TP-G: Privacy protection audit against global collaboration

Audit the activities of the surveilling agents of relevant countries if the digital search warrants are applied or issued invalidly, and if the exchanged information between countries is being used maliciously.

4.5 Propagation to Policy and Global Collaboration

Through the prescriptive design of technologies, consistent policies can emerge. These policies can serve as starting points for analyzing current laws and regulations to identify which policies conform to the current laws, and which should be amended and newly established.

4.5.1 Design of National Policy

PO1: Encourage origin servers and their owning companies to eliminate outgoing malcodes and illegal behavior.

PO1a: Require the originating individual and organization of illegal attacking behavior to be responsible for its behavior and consequences.

PO2: Support blacklist management, which can contribute to preventing repeated illegal behaviors.

PO2a: Support the evaluation of the origin and destination of offensive attacks.

PO3: Support servers being equipped with a victim-initiated reporting procedure.

PO4: Support the research, development, testing, and deployment of the Bright Internet system.

PO5: Require the traceability of origin IP addresses.

PD1: Encourage relevant security software providers to prevent potential zombie computers from being employed by hackers.

PD2: Encourage relevant security agents to conduct proactive surveillance over ISPs or carriers to prevent the delivery of obviously malicious codes that can harm the receivers.

> *PD2a: Allow rule-based identification of surveilling objects by ISPs or carriers.*

PI1: Encourage a two-layered architecture of a pseudonym and a real name to realize identifiable anonymity.

PI2: Require the identifiability of the originator, directly or indirectly, when the valid search warrant requires it.

> *PI2a: Require the organizations who adopt the a posteriori indirect identification method to be responsible for missed identification of originators.*

PI3: Encourage a national standard process of digital search warrant management to be compatible with a global standard procedure.

> *PI3a: Allow the digital search warrant process to be assisted by a rule-based system.*

PP1: Support privacy protection audits against origin and deliverer responsibility procedures.

PP2: Support privacy protection audits against blacklist management.

PP3: Support privacy protection audits against identifiable anonymity procedures.

PP4: Allow a trustworthy third party to audit for the prevention of privacy infringement.

PG1: Recommend adopting privacy protection audits for global collaboration procedures.

4.5.2 Design of Global Collaboration

Likewise, all designs of technologies and policies need to be extended to the global context.

GO1: Encourage origin servers and their owning companies in all countries to eliminate outgoing malcodes and illegal behavior.

> *GO1a: Require the originating individual and organization of illegal attacking behavior to be responsible for its behavior and consequences in all countries.*

GO2: Support global scale blacklist management while maintaining each country's sovereignty.

> *GO2a: Support the evaluation of the origin and destination of offensive attacks on a global scale.*

GO3: Support servers being equipped with a victim-initiated reporting procedure in a global setting.

GO4: Support the research, development, testing, and deployment of the Bright Internet system on a global scale.

GO5: Require the global traceability of origin IP addresses.

GD1: Encourage relevant software providers to prevent potential zombie computers from being employed by hackers on a global scale.

GD2: Encourage relevant security agents to conduct proactive surveillance over ISPs or carriers on a global scale to prevent the delivery of obvious malicious codes that can harm receivers.

> *GD2a: Allow rule-based identification of surveillance objects by ISPs or carriers on a global scale.*

GI1: Encourage a two-layered architecture of a pseudonym and a real name on a global scale.

GI2: Require the global identifiability of an originator, directly or indirectly, when the valid search warrant requires it across borders.

> *GI2a: Require that organizations adopting the a posteriori indirect identification method be globally responsible for the missed identification of originators.*

GI3: Encourage a global standard process of digital search warrant management.

> *GI3a: Allow a global digital search warrant process to be assisted by a rule-based system.*

GP1: Support global privacy protection audits against origin and deliverer responsibility procedures.

GP2: Support global privacy protection audits against blacklist management.

GP3: Support global privacy protection audits against identifiable anonymity procedures.

GP4: Allow a trustworthy third party to conduct audits to prevent privacy infringements in a globally coordinated manner.

GG1: Recommend global privacy protection audits associated with global collaboration procedures.

By deriving a draft of prescriptive international agreements as above, stakeholders can analyze the current international agreements and treaties from this perspective, and can identify what should be amended and/or added. Governmental representatives will also need to consider the Internet Peace Principles and include them in national cybersecurity policies. These issues may be discussed at the Bright Internet Global

Summit. The summit will invite all stakeholders of relevant international organizations, government agencies, researcher groups, and business representatives. During the policy and global collaboration analysis procedure, we may encounter new factors that have not been previously recognized. This kind of recognition will be the point of systematic discussion for the refinement of the initial design.

5 Summary and Concluding Remarks

5.1 Summary

The Bright Internet is proposed as a preventive security paradigm, in contrast with the current self-centric protective security paradigm. For this purpose, the principles of origin responsibility and deliverer responsibility on a global scale are adopted. However, these preventive security-related principles may limit the freedom of anonymous expression. Thus, the principle of identifiable anonymity is adopted in order to protect the freedom of anonymous expression for innocent netizens, also facilitating the traceability and identifiability of criminal origins. In addition, the principle of privacy protection is adopted by requiring audit capabilities that are superimposed on security surveillance. Each of these four principles should be applicable in the context of global collaboration. As such, these five cooperative principles are essential in fulfilling the three seemingly conflicting goals of preventive security, privacy protection, and freedom of expression for innocent netizens.

Most previous research in information systems security and privacy has dealt with the behavioral aspects of individuals and organizations, and has assumed that external attacks on the current Internet platform are uncontrollable. In this regard, the design research of the Bright Internet can be contrasted with these studies, in that it focuses on the societal level of design theory research on a global scale. Since the scale of the target system is enormous, and it is not possible to demonstrate the implemented system at its beginning stages, we adopted two ways of justifying the design principles. One is based on prevention motivation theory, and the other on analogical social norms, which demonstrate that the same spirit is already applied in different contexts in the real world.

To prescriptively design the first version of the Bright Internet 1.0, an outline of the necessary technologies are derived from the principles. The necessary policies are consistently derived from the technology specifications, and are then extended to the need for global collaboration. This proposition can become the starting point toward an agreement of commonly acceptable policies in spite of differences in culture, law, and national security status. As a channel of global communication, AIS has established the Bright Internet Global Summit, where all stakeholders can meet together and exchange ideas.

5.2 Reviews with the Design Science Perspective

To validate the design of the Bright Internet from the perspective of the design science framework (Von Alan, March, Park, & Ram, 2004), we review our work with the seven design science research guidelines, as was also done by Arnott and Pervan (2012) and Gregor and Jones (2007).

1. *Design as an Artifact:* The Bright Internet is aimed at designing an artifact infrastructure, guided by design goals and principles, and Bright Internet 1.0 is a prototypical prescriptive design that encompasses relevant technologies, policies, and global collaborations.
2. *Problem Relevance:* The design principles are basically justified by prevention motivation and analogical social norms. However, further experimental studies will be necessary.
3. *Design Evaluation:* The initial design is evaluated by the justification of principles, consistency between principles and design variables in three constructs of technologies, policies and global collaborations.
4. *Research Contributions:* The primary contribution of Bright Internet research is that it proposes a preventive security paradigm for the Internet, while balancing it with the goals of privacy protection and the freedom of anonymous expression for innocent netizens. For this purpose, we propose and basically justify three goals and five design principles. Based on these principles, we derive the prescriptive design of necessary technologies, policies and global collaborations.
5. *Research Rigor:* Our analysis of prevention motivation theory and analogical social norm theory justifies the principles. The principles should be further evaluated by subsequent survey studies, and it will also be necessary to explore the effect of cultural differences. Furthermore, consistent designs will emerge from prescriptive technologies, policies, and global collaborations.
6. *Design as a Search Process:* There can be more than one design with the principles, and competition between designs will create a more cost-effective design. We designed the Bright Internet 1.0; however, we expect that alternative designs and technologies will emerge and compete. Diverse business models will also create the application-specific deployment. Discussion among stakeholders will refine the design toward global consensus.

7. *Communication of Research:* Research on the Bright Internet requires the collaboration of diverse academic disciplines from technology, system building, policy, global collaboration and business practice. This paper will open a common ground of discussion among them.

5.3 Extended Research Opportunities

Bright Internet research can trigger research opportunities from various angles. It requires research about technologies, business models, policies, and global collaborations. Typical technological issues for preventive security are origin- and deliverer-driven screening and victim-driven traceability and identifiability, reconciliation of identifiability and anonymity, and auditing for privacy protection. For the validation of principles and technologies, wide behavioral research in experimental settings or empirical test beds must be conducted in different social and global contexts. Prevention motivation theory and analogical social norm theory can be tested empirically. The behavioral issues on individual- and organization-level studies can be explored even before the model is deployed in the real world, allowing researchers to design the future. In this manner, a virtuous cycle of behavioral scientific research topics can emerge, based on design science research.

Acknowledgments

This research aims to fulfill the vision of the AIS Bright ICT Initiative, and is funded by the KAIST Bright Internet Research Center, EEWS Research Center (Grant for Climate Change Global Hub Research), and the Institute for Information & Communications Technology Promotion in Korea. The Heinz College of Carnegie Mellon University and the School of Management at Xi'an Jiaotong University have also supported this research. We are grateful to the research partners of the Bright Internet projects in Korea, China, and the USA. Particular thanks are extended to President Sanghoon Lee of the Electronics and Telecommunications Research Institute (ETRI) and Director Chaesub Lee of ITU's Telecommunication Standardization Bureau for their insightful partnership from the advent of the Bright Internet. Discussions with Professor David Farber have awakened the importance of the human rights aspect.

References

Adomavicius, G., Bockstedt, J. C., Gupta, A., & Kauffman, R. J. (2008). Making sense of technology trends in the information technology landscape: A design science approach *MIS Quarterly, 32*(4), 779-809.

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.

Arnott, D., & Pervan, G. (2012). Design science in decision support systems research: An assessment using the Hevner, March, Park, and Ram guidelines. *Journal of the Association for Information Systems, 13*(11), 923-949.

Baskerville, R. L., Kaul, M., & Storey, V. C. (2015). Genres of inquiry in design-science research: Justification and evaluation of knowledge production. *MIS Quarterly, 39*(3), 541-564.

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.

Bi, J. (June, 2016). IPv6 traceable anonymity for the Bright Intern et. *Workshop for Bright Internet.* Conducted at the Pacific Asia Conference on Information Systems, Chiayi, Taiwan.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-548.

Chaturvedi, A. R., Dolk, D. R., & Drnevich, R. L. (2011). Design principles for virtual worlds. *MIS Quarterly, 35*(3), 673-684.

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.

Cho, D. & Lee, J. K. (2016). Social norms about the principles of the Bright Internet (KAIST working paper).

Coleman, J. (1990). *Foundations of social theory*. Cambridge, MA: Harvard University Press.

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.

Elster, J. (1989). Social norms and economic theory. *Journal of Economic Perspectives, 3*(4), 99-117.

ERP (2014). European recycling platform celebrates a landmark recycling milestone of 2 million tonnes of WEEE [Media release of European Recycling Platform]. Retrieved from http://www.erp-recycling.org/wp-content/uploads/sites/13/2013/11/ERP-Europe-Recycles-2-Million-Tonnes-of-WEEE-Corporate-140214.pdf.

Forrest, C. (2016). Report: 80% of businesses can't properly manage external cyber attacks. Retrieved from http://www.techrepublic.com/article/report-80-of-businesses-cant-properly-manage-external-cyber-attacks.

Gregor, S. & Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. *MIS Quarterly, 37*(2), 337-355.

Gregor, S., & Jones, D. (2007). The anatomy of a design theory. *Journal of the Association for Information Systems, 8*(5), 312-335.

Herath, T., & Rao, H. R. (2009a). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125.

Herath, T., & Rao, H. R. (2009b). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154-165.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in Information Systems research. *MIS Quarterly, 28*(1), 75-104.

Horst, T. (2014). One-day wonders: Here today, gone tomorrow. Retrieved from https://www.bluecoat.com/security-blog/2014-08-26/one-day-wonders-here-today-gone-tomorrow.

Hsu, J. S. C., Shih, S. P., Hung, Y. W., & Lowry, P. B. (2015). The role of extra-role behaviors and social controls in information security policy effectiveness. *Information Systems Research, 26*(2), 282-300.

IFIP (2015). The 2015 Dewald Roode workshop on Information Systems security research. Conducted by IFIP 8.11/WG11.13, Newark, Delaware.

IGF (2016). Internet Governance Forum. Retrieved from

https://en.wikipedia.org/wiki/Internet_Governance_Forum.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly 34*(3), 549-566.

Kolthof, D. (2015). Crime in the cloud: An analysis of the use of cloud services for cybercrime. Paper presented at the Student Conference on IT, Enschede, The Netherlands.

Korea Herald. (2013, August 23). Constitutional court rules real-name policy online unconstitutional. Retrieved from http://www.koreaherald.com/view.php?ud=20120823001079.

Krebs, B. (2015). Who's attacking whom? Realtime attack trackers. Retrieved from http://krebsonsecurity.com/2015/01/whos-attacking-whom-realtime-attack-trackers.

Kuecheler, W. M. & Vaishnavi, V. (2012). A framework for theory development in design science research: Multiple perspectives. *Journal of the Association for Information Systems, 13*(6), 395-423.

Lawson, K. (2012). Ask the expert: Can a botnet really turn my computer into a zombie? [Blog post]. Retrieved from http://blog.privatewifi.com/ask-the-expert-don%E2%80%99t-become-a-botnet-zombie

Lee, H. & Shao, M. (2009). The European recycling platform: Promoting competition in e-waste recycling [Case study GS-67, Stanford Graduate School of Business]. Retrieved from https://www.gsb.stanford.edu/faculty-research/case-studies/european-recycling-platform-promoting-competition-e-waste-recycling.

Lee, J. K., & Kwon, S. B. (1995). ES*: An expert systems development planner using a constraint and rule-based approach. *Expert Systems with Applications, 9*(1), 3-14.

Lee, J. K. (2002). Internet Auction Ltd.'s lesson. *Lecture Note on eAuction Business and Fraud Protection*, Jae Kyu Lee at College of Business, KAIST.

Lee, J. K. (2015). Research framework for AIS grand vision of the Bright ICT Initiative. *MIS Quarterly, 39*(2), iii-xii.

Lee, J. K. (2016a). Invited commentary—Reflections on ICT-enabled Bright Society research. *Information Systems Research, 27*(1). Retrieved from http://dx.doi.org/10.1287/isre.2016.0627.

Lee, J. K. (2016b). *Can the Bright Cloud be a business model?* Keynote speech presented at the Ninth IEEE/ACM International Conference on Utility and Cloud Computing, Shanghai, China.

Mitra, S., & Ransbotham, S. (2015). The effects of vulnerability disclosure policy on the diffusion of security attacks. *Information Systems Research, 26*(3), 565-584.

Nagin, D. S. (2013). Deterrence in the twenty-first century. *Crime and Justice, 42*(1), 199-263.

Nygren, E. (2015). The three years since world IPv6: Strong IPv6 growth continues [Blog post]. Retrieved from https://blogs.akamai.com/2015/06/three-years-since-world-ipv6-launch-strong-ipv6-growth-continues.html.

Oetzel, M. C., & Spiekermann, S. (2014). A systematic methodology for privacy impact assessments: A design science approach. *European Journal of Information Systems, 23*(2), 126-150.

Orlowski, A. (2016, September 15). EU ends anonymity and rules open Wi-Fi hotspots need passwords. *The Register*. Retrieved from http://www.theregister.co.uk/2016/09/15/eu_ends_anonymity_and_rules_open_wifi_hotspots_need_a_password; retrieved October 12, 2016).

Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go? *MIS Quarterly, 35*(4), 977-988.

Peffers, K., Tuunanen, T., Rothenberger M. A., & Chatterjee, S. (2007). A design science research methodology for Information Systems research. *Journal of Management Information Systems, 24*(3), 45-77.

Rowland, C. H. (2002). Intrusion detection system. *US Patent 6405318 B1*.Washington, DC: U.S. Patent and Trademark Office

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology, 91*(1), 93-114.

Rossem, C. (2008). Individual producer responsibility in the WEEE directive: From theory to practice? (Doctoral dissertation, The International Institute for Industrial Environmental Economics, Lund University, Lund Sweden). Retrieved from http://portal.research.lu.se/ws/files/5603015/1266800.pdf.

Shcherbakova, T., Vergelis, M., & Demidova, N. (2015). Spam and phishing in Q3 2015, Kaspersky Lab. Retrieved from https://cdn.securelist.com/files/2015/11/Q3-2015_Spam-report_final_EN.pdf.

Shin, Y. Y., Lee, J. K. & Kim, M. C. (2018). Preventing state-led cyberattacks by the Bright Internet and Internet Peace Principles. *Journal of the Association for Information Systems, 19*(3). In press.

SIGSEC (2015). Pre-ICIS workshop on information security and privacy. Conducted at the International Conference on Information Systems, Fort Worth, Texas.

Simon, H. (1996). *The science of the artificial* (2nd ed.). Cambridge: Massachusetts Institute of Technology Press.

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.

Turban, E., King, D., Lee, J. K., Liang, T, & Turban D. C. (2015), *Electronic commerce: A managerial and social network perspective* (8th ed.). New York, NY: Springer.

United Nations (2016). Article 1: The purpose of the United Nations. Retrieved from http://www.un.org/en/sections/un-charter/chapter-i/index.html.

Virvilis, N. & Gritzails, D. (2013). The big four—What we did wrong in advanced persistent threat detection? In *2013 International Conference on Availability, Reliability and Security* (pp. 248-254), IEEE.

Von Alan, R. H., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research, *MIS Quarterly, 28*(1), 75-105.

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.

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems, 18*(2), 101-105.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly, 37*(1), 1-20.

WSIS. (2005). Tunis Agenda for the information society. Retrieved from http://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html.

About the Authors

Jae Kyu Lee has been a professor and chair professor at the Korea Advanced Institute of Science and Technology since 1985, and is currently professor emeritus of KAIST and chair professor at Yonsei University in Seoul. He was also a distinguished visiting professor at Heinz College at Carnegie Mellon University in 2016-17 and is an honorary chair professor of Xi'an Jiaotong University. He is a fellow and past president of the Association for Information Systems and is founder of the Bright Internet. He was a conference co-chair at the International Conference of Information Systems, 2017. He received his PhD from the Wharton School at the University of Pennsylvania.

Daegon Cho is an assistant professor of information systems in the College of Business at Korea Advanced Institute of Science and Technology in Seoul, and is the director of the Bright Internet Research Center at KAIST. He received his PhD from the Heinz College at Carnegie Mellon University. Prior to joining KAIST, he was a faculty member at Pohang University of Science and Technology (POSTECH). His research topics are economics of information systems, business analytics, information security and privacy, and healthcare/energy IT.

Gyoo Gun Lim is a professor of MIS at the Hanyang University Business School. Before joining Hanyang University, he was an associate professor at Sejong University and a researcher with Samsung Electronics and Korea Telecom. He was a Fulbright visiting scholar at the Hass Business School at U.C. Berkeley in 2012. He received an award from the Korea Ministry of Information and Communication for his contribution to Korea SW industry in 2007 and an award from the Korea Ministry of Knowledge Economy for his contribution to Korea IT innovation in 2009. His current research interests include IT service, innovative business models, e-business, and intelligent information systems.