GUEST EDITORIAL

Research Framework for AIS Grand Vision of the Bright ICT Initiative

By: **Jae Kyu Lee**
President, Association for Information Systems (2015–2016)
Korea Advanced Institute of Science and Technology
Seoul, Korea
jklee@business.kaist.ac.kr

The Internet has become a minefield of crime, fakes, and terror perpetuated by anonymous users on a global scale. The security burden of protecting organizations is becoming increasingly difficult and costly, and this burden cannot be lessened under the current Internet protocol. In order to fundamentally solve these side effects, the Council of the Association for Information Systems (AIS) has adopted a grand vision of an ICT-Enabled Bright Society (in short, the *Bright ICT Initiative*). With the goal of preventing undesirable activities on the Internet, diverse issues can be investigated using a bottom-up perspective. Scholars are beginning to examine the concept and various approaches with the support of the AIS conferences and the information system journals. However, a unique approach and fundamental solution must be identified in order to drastically eliminate the negative side effects of these adverse online activities. In order to achieve this, four principles are proposed that will provide the foundation of the framework for a new and safer Internet platform, the *Bright Internet*, while protecting users' privacy at an appropriate level. The proposed principles are *origin responsibility, deliverer responsibility, rule-based digital search warrants,* and *traceable anonymity*. This endeavor requires the investigation of technologies, policies, and international agreements on which new business models can be created.

Introduction: Negative Side Effects Caused by the Internet

The proliferation of the Internet worldwide has resulted in over 929 million websites and 3.1 billion users as of April 15, 2015 (Internet Live Stats 2015). Smart phones have pushed the expansion of the mobile Internet to 1.64 billion users with a 25 percent increase in 2014 (eMarketer 2014). Internet-based commerce has become part of daily life and more personalized services have become possible due to ubiquitous data collection and big data analysis (Craig and Ludloff 2011). The future of the "Internet of Things" (IoT) will further expand the penetration of the Internet in unimaginable ways. As such, Internet-based information and communication technologies (ICTs) have become an inevitable tool in daily life around the world.

The benevolent intention of the Internet is to enable global communication virtually distance-free and to make the life and business of global inhabitants more convenient and happier. To this end, the anonymity of Internet access has been supported to enhance the convenience and freedom of expression.

However, the Internet today is abused by perpetrators of anonymous cyber crimes and terror at an intolerable scale. According to a recent report, 378 million users are victims of cyber crimes every year through attacks by spam, malware, viruses, hacking, scams, fraud, and theft. Furthermore, 38 percent of mobile Internet users have experienced cyber crimes, with an average cost-per-victim of cyber crime is $298, totaling $113 billion in 2013 (Symantec 2013). Moreover, 56 billion spam messages are sent each day, and 68 percent of e-mails are considered to be spam (Kohavi 2014), with 90 percent of spam being sent from servers compromised by hackers (Rao and Reiley 2012). An even scarier statistic is that 71 percent of host names exist for only 24 hours, and the top- ten most prolific creators of these "one day wonders" are leading pornography websites on Google, Amazon, and Yahoo (Blue Coat 2014). Distributed denial of service (DDoS) attacks with higher bandwidths damaged 60 percent of companies in North America in 2013, a 71 percent increase from 2012 (Neustar 2014). These illegitimate activities use up a big chuck of Internet capacity.

As observed above, the Internet has become a chaotic superhighway without appropriate traffic lights or police, resulting in the widespread commission of cyber crimes world-wide. National telecommunication, energy, banking, and transportation infrastructures have become vulnerable to cyber terror, and the Internet has become the new battlefield rather than contributing to peaceful life across borders (Singer and Fridman 2014). For example, a nuclear power plant has already been hacked and threatened by terrorists. It is easy to imagine that, in the not-so-distant future, malicious hackers could cause traffic accidents by taking control of self-driving cars. What will the world be if we do not find a solution to Internet-based crime? Will our current quest for higher speeds and more memory make a difference? The Internet cannot progress further without a fundamental solution that will eliminate the sources of basic risks.

The Sony Pictures hack demonstrated that individual servers are responsible for the protection of their own content without additional support or protection from national or global governance (Savor 2014). In order to reduce potential risks at a fundamental level, current security principles need to be changed. This responsibility should not be borne by the destination servers alone.

Most fraud and crime on the Internet are committed by anonymous entities (Levmore and Nussbaum 2010). Cyber bullying is committed by anonymous users who tend to express themselves using harsh words and rude opinions (Sticca and Sonja 2013). Should there be a limitation on anonymous freedom of expression so that innocent victims could be better protected?

Mere investigation of business information systems can no longer make people and businesses happier and more prosperous. That is why the AIS has adopted the grand vision project for an ICT-enabled Bright Society (in short, the Bright ICT Initiative). More attention should be given to solving the problems that the Internet has caused and the societal policy problems that are the ecology of businesses (Deibert 2013). We also have to pay more attention to solving the global problems caused by the inherent nature of the Internet.

This editorial reviews the current progress of the Bright ICT Initiative, and proposes a vision for Bright Internet that adopts a set of principles that can make the Internet safer while protecting reasonable levels of privacy (Solove 2008). The four principles proposed for beginning stage are *origin responsibility, deliverer responsibility, rule-based digital search warrants*, and *traceable anonymity*. The deployment of the Bright Internet requires the development of new technologies, policies, and international agreements based on these principles. New research and business opportunities will expand ways this vision can be achieved and new rules for the Internet will be created.

Open Issues Toward Bright ICT Research

In this context, the IS research community should identify problems and devise solutions to make our future society brighter and safer. What are the key issues that need to be investigated? What principles can significantly alleviate the troubles that plague the current Internet platform? How can privacy and security be balanced at company and national levels? What form should the architecture and protocol of the Bright Internet platform take? What should be the national policy to balance security and privacy? What should the international agreement and global governing structure be in order to manage the interests of global stakeholders? These are the research questions that we have to investigate and they are profound opportunities for IS researchers.

The spectrum of problems is broad and a variety of expertise and research perspectives are needed. Research topics on identifying the problems and developing solutions that will enable a brighter future for the Internet are open. Significant research opportunities for diverse researchers can be created in this pursuit. Typical topics include, but are not limited to, the following:

1. Security: fraud and cyber crimes, vulnerability to cyber terror
2. Privacy: abused anonymity and privacy infringement, information leakage (Solove 2011)
3. Addiction: excessive use of communication and excessive gaming
4. Social dynamics: misleading minorities in cyber space may impact future political systems (Deibert et al. 2010)
5. Green IT: use of IT to reduce energy consumption and carbon emissions

These issues are challenging, but they can become opportunities. First of all, we should identify the major sources of risks and propose approaches that can drastically eliminate the problems. Without the pursuit of significant contributions, the announcement of a grand vision is meaningless. There is a need for foundational principles to reengineer the Internet platform.

In order to encourage research on Bright ICT, the AIS Council has organized a special task force to promote the initiative in a sustainable manner. The members of task force are Jae Kyu Lee, Jane Fedorowicz, Helmut Krcmar, Cynthia Beath, Allen Lee, Joey George, Niels Bjørn-Andersen, and Ramayya Krishnan (AIS 2015). The task force encourages the organization of panels and workshops at AIS conferences to exchange ideas about the vision for the Bright ICT Initiative. The IS community needs to understand what the vision is, what can be done, and what the opportunities are for IS researchers.

The first panel on the Bright ICT was organized at ICIS 2014 in Auckland, New Zealand. The inaugural panel was hosted by Jane Fedorowicz (Immediate Past President of AIS), Helmut Krcmar (President of AIS), Jae Kyu Lee (President-Elect of AIS), Ramayya Krishnan (Dean of the Heinz College, Carnegie Mellon University), and Kevin Desouza (AIS Vice President of Communications, Arizona State University). These panelists presented the motivation and background of the Bright ICT Initiative and explained why it is necessary for the AIS community to take note and to work together. This panel also presented the research topics in progress at the participants' universities, and Jae Kyu Lee presented the framework approaches of the Bright ICT Initiative that make it unique and fundamentally different from current approaches. There was consensus that the Bright ICT Initiative needs to allow diversity in order to accommodate diverse issues and interests, but that a core, concrete issue should be defined to create fundamental value for society. This framework is described in the next section under the concept of the Bright Internet.

AIS, through its conferences, will organize special panels to discuss the next steps of the initiatives and regional interests. In the beginning stage, brainstorming the diverse views will assist in the identification of research issues. At AMCIS 2015 in Puerto Rico, the panel will discuss "The AIS Grand Vision Project: What, Why, and How." Jane Fedorowicz (Bentley University) will moderate with panelists Gwanhoo Lee (American University), Richard Watson (University of Georgia), Ritu Agarwal (University of Maryland), Ping Zhang (Syracuse University), and Jae Kyu Lee (KAIST). The panel will investigate why the problems under the Bright ICT Initiative are compelling and important, and how action items and opportunities for AIS members can be identified.

At ECIS 2015 in Munster (Germany), a panel titled "European Perspectives of the Bright ICT Initiative with Global Reach" will be moderated by Ferdinando Pennarola (AIS ICIS Representative, Italy) with panelists Helmut Krcmar (Germany), Henk G. Sol (Netherlands), Niels Bjørn-Andersen (Denmark), and Jae Kyu Lee (Korea).

The ECIS panel will contrast the vision of the Bright ICT Initiative with the United Nations' eight Millennium Development Goals that aim to solve the conflicting, unjust, and unsafe problems of today. The panel seeks to identify the stream of relevance of IS research in the Bright ICT context, raising the question of whether IS research endeavors are returning value to society. At the same time, the panel aspires to raise new perspectives regarding the value of IS research to society and the types of changes necessary. The Bright ICT Initiative is regarded as an opportunity to increase the value of our research outcomes.

PACIS 2015 in Singapore will also organize a panel with the Asia Pacific perspective. Jungpil Han (National University of Singapore) will moderate the panel with panelists from Japan (Masaki Hirano, Waseda University), Singapore (Steven Miller, Singapore Management University), New Zealand (Michael Myer, Auckland University), and Korea (Jae Kyu Lee, KAIST).

In order to encourage journal publications on the issues around the Bright ICT Initiative, a special issue of the *Journal of AIS* will be guest edited by Alessandro Acquisti (Carnegie Mellon University) and Wonseok Oh (KAIST). In addition, *Information System Research* is planning a special section focused on Bright ICT issues, and other leading journals are also considering special issues. The issues of interest include, but are not limited to, the following:

- Responsibilities of cyber security and obligations of Internet platform providers
- Design of traceable anonymity that secures both privacy and security
- Economics of computer security and privacy
- Legal aspects of Internet crimes and privacy violation
- Effects of privacy concerns on online consumer behaviors
- Big data analytics and privacy concerns
- Exploration of cyber bullying and online harassment in social networking sites
- Social and political conflicts in online communities and social networks
- Assessments of digital addictions to games and social networking sites
- Potential risks of an IoT-enabled society

At ICIS 2015 in Fort Worth, Texas, AIS will sign an agreement with the International Telecommunication Union (ITU) to formally collaborate on research and implementation. Furthermore, there will be a dedicated workshop on the development of globally coordinated research projects with the topics of Bright ICT. Through these endeavors, researchers will begin to investigate the important issues and publish papers at conferences and in journals.

Principles for the Bright Internet Protocol

As mentioned earlier, the core research topics and approaches of the Bright ICT Initiative need to be defined in order for society to appreciate its fundamental value and distinctive approach. For this purpose, four principles are proposed to construct the framework of the Bright Internet Protocol: origin responsibility, deliverer responsibility, rule-based digital search warrants, and traceable anonymity.

In order to explain the architecture of the Bright Internet Protocol, the typical architectures of corporate security systems currently in use should be contrasted (Cobb 2003). Corporate information systems are responsible for the protection of their own servers and users. The servers must protect themselves from all types of external attacks and illegal leakages. Therefore, the full architecture of a corporate security system consists of protection against distributed denial of service (DDoS) attacks, firewalls for authentication and virtual private networks (VPNs), intrusion protection systems with content filtering capabilities, protection against advanced persistent threats (ATPs) that fabricate attacks using multiple phases of breaking into a network to avoid detection, mail security systems, digital rights management, and data leakage prevention. In order to protect users of the servers, system operators merely alert users not to click on items that contain potentially hazardous viruses or phishing attempts.

Nevertheless, the current architecture cannot completely protect the security of the systems even though it is very expensive. Furthermore, small businesses and individuals cannot afford the expertise or cost. Thus, two fundamentally new principles—the *principle of origin responsibility* and the *principal of deliverer responsibility*—need to be adopted. In order to contrast these two principles with the current implicit principle, the current principle can be called the *principle of destination responsibility*—that is, the responsibility of security is borne by the destination servers, the servers to which the spam and malicious messages are delivered.

Principle 1: Origin Responsibility

When the responsibility of security risks is borne by destination servers, the origin servers do not have any significant incentives to prevent sending undesirable content. This phenomenon enables the creation of malicious content without control. In order to reduce the intentional creation or negligence of disseminating harmful or wasteful content from origin servers, the principle of origin responsibility should be adopted. The primary purpose of this principle is to motivate the origin servers to prevent sending malicious messages and thus fundamentally eliminate the sources of spam.

The principle requires that outgoing mail at the origin server be monitored. Because approximately 68 percent of e-mails are spam, the wasted load of the Internet infrastructure could be significantly reduced and the malicious side effects of spam prevented. Therefore, implementation of the principle requires methods that reduce the overhead of monitoring outgoing mail without jeopardizing user privacy. An efficient and effective protocol can be designed by utilizing feedback from users at destination servers who were affected by the spam. In this regard, both technology and policy research for the implementation of Principle 1 can be designed.

A reference model for the principle of origin responsibility can be found in the waste management of electronic and electrical equipment. The Directive on Waste Electrical Electronic Equipment (WEEE Directive) (European Commission 2015) adopted the *principle of individual producer's responsibility* to motivate producers to reduce harmful waste during the design and production stages of their product lifecycle. In order to implement this principle, a third party business of waste collection emerged such as the European Recycle Platform (ERP 2015), which collected 2 million tons of electronic waste in 2014. The competition of the third party services has significantly reduced the cost of waste collection from €0,70 in 2005 to less than €0,075 in 2007 (Shao 2009). As such, the principle of origin responsibility for the Internet has the potential to significantly reduce the dissemination of harmful spam from its origin.

The level of harmfulness of origin servers can be measured using the *Bright ICT Index*, and the value can be calculated through counting the number of spam messages and their damage. The behavior of the origin servers can be easily measured through monitoring reports from the affected recipients if the Bright Internet Protocol supports the reporting procedure. The logic of penalizing the harmful effect from the offending servers can be derived using the Bright ICT Index. An experimental test bed can be established and the empirical data of the indices can be measured. In the first stage of the experiment, the influence of the information disclosed regarding the indices on the behavior of origin servers can be analyzed. He et al. (2014) simply measured the ranking of harmfulness that corresponds to a basic type of Bright ICT Index. However, the suitable definitions for the Bright ICT Index need to be further investigated.

The concept of origin should be studied in at least four layers: *user, server, company*, and *country*. If the owner of a server does not behave ethically, the governing country should enforce measures to prevent the unethical behavior. If the country does not establish a suitable policy to enforce ethical behavior of companies in their sovereign territory, the global governing body of the Bright Internet should encourage the country to behave as a good global citizen. A global governance structure is required for which international agreement is necessary.

It will be necessary to charge penalties and taxes in alignment with the harmful effect within a country and tariffs between countries. For the international implementation of tariffs, the global governing body will require an accounting capability. Thus, the principle of origin responsibility can trigger the development of necessary technologies, national policies, and international agreements that are essential to fulfill the goal. Eventually, the global governing organization could adopt common standards to enable the operations of the Bright Internet Protocol to be safer and more efficient. Then, a vast business models for the Bright Internet will be created and a new industry will emerge.

Principle 2: Deliverer Responsibility

Although the principle of origin responsibility can significantly reduce spam, it will not be easy to control the malware in compromised computers because 90 percent of spam is created by compromised computers. DDoS attacks are also created by millions of zombie computers. Telecommunication carriers also deliver SMS and voice phishing without knowing the content and the subsequent harmful effects. Therefore, it is proposed that surveillance of deliverers be allowed in an attempt to prevent the delivery of harmful messages. However, there is a question about whether the deliverers should be allowed to monitor messages and packet content in order to filter the fraudulent content. Therefore, the surveillance should be conducted without infringing the privacy of innocent netizens by adopting an advanced mechanism such as a rule-based digital search warrant, which is explained in detail in the third principle.

There are two perspectives on the position of deliverers. On the one hand, the unintentionally infected deliverers that became zombies can be regarded as victims. On the other hand, from the final victims at the destination server's perspective, the zombies are accomplices of the malicious originators. Therefore, zombies should not cooperate with malicious originators by neglecting their responsibility to not hurt other servers, even though their part in the attack might have occurred unintentionally. The deliverers should have checked their own systems to detect whether they were infected with malware prior to sending spam messages. In order to motivate the elimination of the potential risks caused by the deliverers such as routers, zombie computers, and carriers, the deliverers should bear the corresponding responsibility. This is the notion of Principle 2: deliverer responsibility.

In this regard, deliverers have a legal responsibility to prevent plausible harmful attacks and they cannot be willfully negligent. An analogy to illustrate this point is that a passenger should not blindly deliver drugs through carrying a stranger's bags. Ignorance or negligence cannot be a justification to exempt one from responsibility.

Social consensus is necessary in order to establish an adequate policy for the implementation of the principle of deliverer responsibility. We believe the potential benefit of implementing deliverer responsibility is inevitable as far as the schemes of protecting privacy can be developed. Therefore, this principle is regarded as the direction in which the Bright Internet Protocol should proceed. The concept of solution tools for the implementation of deliverer responsibility will be similar to those for the origin responsibility. However, the scale of the tools will become very large and the principle will significantly change the business models of deliverers.

Principle 3: Rule-Based Digital Search Warrants

The implementation of deliverer responsibility requires real-time surveillance of packets by content and/or by user name (Stotz and Sudit 2007). This may infringe on the privacy of platform users, and the deliverer may not be legally allowed to execute this surveillance (Nissenbaum 2010). We argue that the privacy of innocent users can be protected if the *principle of rule-based digital search warrants* is adopted. In order to detect the intention of terror and fraud, billions of messages should be inspected daily. Because it is not possible for humans to inspect all messages, a software agent that is permitted real-time surveillance of all messages is needed, but it should only be allowed to access the content if the message violates the rules that are identified by the digital search warrants issued by authorities in advance.

Using the scheme of Principle 3, the privacy of innocent netizens will not be infringed on by government. Thus, the advantages and disadvantages of monitoring the messages can be analyzed by balancing the benefits for national security with privacy protection. We believe that the benefit of surveilling messages using rule-based digital search warrants is significantly greater than the risk of infringing the privacy of innocent netizens.

An example of the need for implementation of rule-based digital search warrants can be found in messenger service sites such as Kakao Talk, a messenger service based in Korea. Kakao Talk has 140 million users in 230 counties. The Korean government issued search warrants to the servers in order to protect national and social security. However, the operator of the service opposed the implementation of these search warrants in order to maintain the privacy of users. The company was afraid that their users might stop using their service if the government began monitoring messages because users might perceive this monitoring as an intrusion on their privacy. This type of conflict is a common issue that needs to be resolved for the many similar telecommunication companies providing message services.

This mechanism is analogous to the inspection process at airports. Passengers tolerate an acceptable level of inconvenience in order to prevent the risk of terror. Another analogy is the deployment of closed circuit television in various locations in order to prevent crime and to detect criminals. It is acceptable to keep private information for a certain time period and delete it unless a crime is detected. If no crime is detected, the citizen's private information will not be infringed.

Because citizens are concerned that governments may abuse their private information, the software agent should be certified to conform to its purpose and to be independent of the government (Greenwald 2014). Civilian organizations may participate in the inspection of software functions and the legitimate use of software agents. In the cross-border context, international agreements to adopt software agents will be required. However, it will be unavoidable that different countries might apply different rules depending upon the national policy and security situation.

Principle 4: Traceable Anonymity

Anonymity is allowed in order to guarantee freedom of expression. However, criminals almost always hide behind anonymity. When the hackers attacked Sony Pictures, police could not quickly trace the originating servers and hackers, because the Internet protocol does not effectively support tracing the origin and real names. Thus, when an online crime is detected, the digital search warrant should immediately authorize tracing the source (Baba and Matsuda 2002) and the real names of hackers in order to prevent the abuse allowed by anonymity. Technologies for selectively traceable anonymity have been studied by von Ahn et al. (2006). However, implementation needs the permission by laws that allow tracing real names when a crime is detected.

In Korea, the Constitutional Court determined that the law that required real names for large-scale portal site users is unconstitutional based on the logic that the law breached the constitutional freedom of expression (Yonhap News Agency 2012). However, this judgment is not intended to permit untraceable anonymous crimes on the Internet. Two layers of anonymity need to be distinguished: *freedom of expression* and *prevention of anonymous crime*. At the layer of freedom of expression, anonymity of citizens should be protected. However, once a violation of law is detected, the real name of the anonymous user should be traceable (Wondracek et al. 2010). Adoption of Principle 4 is necessary in order to protect national security and solve crimes.

Determining the adequate level of anonymity and security is a debatable issue. The notion that traceability is permitted only when a user has committed a crime can be implemented by activating the corresponding digital search warrant when the crime is

detected. As such, it would be effective to combine traceability with rule-based digital search warrants in order to protect both the privacy of innocent users and national security.

In order to assure real names at the interface of the physical world, some schemes need to be designed that certify the traceability of users' real names even in public access areas such as Internet cafés and Wi-Fi. If the user's real name is not assured, the access service providers should take responsibility when illegal activities occur. The service provider would then become cautious about allowing potentially harmful access to their network.

We need to develop policies and technologies for the implementation of traceable anonymity. Cross-border cooperation is also necessary if the crime is originated from another country. Global governments should cooperate in order to prevent the emergence of cyber crime havens that allow anonymity without traceability.

The Bright Internet Protocol and Governance Structure

In order to prevent negative side effects to the Internet, a new platform needs to be created that can resolve global issues inherent in the TCP/IP protocol (Lee and Knight 2005). We propose that the Bright Internet Protocol, consisting of the four principles described earlier (origin responsibility, deliverer responsibility, rule-based digital search warrants, and traceable anonymity) be adopted. In the first stage, only the two principles of origin responsibility and deliverer responsibility will be implemented, focusing on protection from spam e-mails, short messages services (SMS), and DDoS attacks in order to solve the most urgent problems. Once various protocols fulfilling the principles have been investigated and tested, the industry will be able to select the best set of standards to be adopted by global Internet users. However, the Bright Internet Protocol must be designed with a long-term perspective including the four principles. Additional principles such as *addiction prevention* and *child protection* can be added gradually once the foundation of the Bright Internet is established.

The implementation of the Bright Internet needs to cover the development of intelligent security technologies, the establishment of national policies, and the establishment of a global governance body, namely the *Bright Internet Global Governance (BIGG) Center*. The BIGG Center needs to establish the global technical standards, internationally acceptable common policies, the metrics of *Bright ICT Indices*, a disclosure policy for the indices, and accounting systems in order to impose penalties and tariffs for harmful behaviors of originating companies and countries.

The Bright Internet platform will make the future Internet safer and more peaceful, and it will create significant new business opportunities while profoundly preventing the origin of risks. This endeavor will create a multitude of new business model opportunities through realizing the next generation of the Internet with minimal negative side effects. New rules for the Internet civilization will be created.

The opportunity to work toward the Bright Internet is open to all institutions and countries. KAIST is now proposing the establishment of the Bright Internet Research Center to specifically design the principles, necessary technologies, policies, and international governance. This center will contribute to the initiation of globally coordinated research on designing the protocol and operational structure of the BIGG Center, which will operate the protocol.

This raises the question of who should own and work for the BIGG Center. Should it be independent or owned by an existing institution such as Association for Information Systems, the International Telecommunication Union, the United Nations, or Internet Corporation for Assigned Names and Numbers? This question is open to exploration. AIS intends to organize workshops to discuss these issues, and they plan to organize a global summit of Bright Internet in cooperation with ITU in order to investigate the most desirable governance structure and standards for all participating stakeholders. We need to learn lessons from the history of Internet governance.

Bright ICT Indices and Territorial Responsibility

The need for Bright ICT Indices was mentioned briefly earlier. The metrics for the Bright ICT Indices must be measured at the levels of individual users, servers, companies, and countries in order to evaluate the degree of harmful behavior on the Internet.

In order to motivate the reduction of harmful behavior, the index information should be disclosed to the public and relevant stakeholders. It might also be included in the annual reports in stock markets across the world. The Bright ICT Index between companies and countries can be converted to penalty amounts to pay or to be paid by the corresponding companies and countries. In order to calculate the indices, the definition of indices should be specified, and the calculation method of penalties and a clearing mechanism need to be established as commonly agreed standards.

He et al. (2014) have monitored the amount of spam e-mails from 8,000 companies globally, and they measured the impact as a ranking of harmfulness. They also tested whether the disclosure of the ranking information contributed to reducing the emission of spam email. Stefan Savage, professor of Computer Science and Engineering at the University of California, San Diego, studied the effect of charging taxes on reducing spam e-mails (Farrow 2011).

If the index value is announced at least once per year and shared globally, new consulting businesses for the measurement and dissemination of the indices will emerge to help corporations and countries reduce the side effects of their information systems. In order to calculate the responsibility of one country to another, the accumulated penalty of the servers in the country should be calculated. If a company does not pay for the penalty legitimately, the sovereign government should pay the penalty on behalf of the company in order to motivate the country to establish appropriate internal enforcing policies. Furthermore, the BIGG Center needs to establish a commonly agreed framework of calculating penalties, taxes, and tariffs in order to motivate the global stakeholders of the Bright Internet.

Holistic Approach Combining Technology, Policy, and Business Models

The current research paradigms for cyber securities are fragmented by the different expertise of different communities. In general, the technology community only researches technical issues, while the policy community only researches policy issues, and there is typically a lack of close communication between these communities. It is not easy to research across the boundaries due to the knowledge barriers between the two. However, in order to design the future of the Bright Internet, we must design the future holistically to encompass technology, policy, international agreements, and business models to make it succeed.

Thus, the following research questions need to be investigated while considering the relationship among the questions holistically:

1. What are the technologies necessary to implement the principles of the Bright Internet Protocol effectively and efficiently?
2. What types of current national policies prohibit the implementation of the principles in practice, even though the technologies may become available? What current policies should be revised and what policies should be established in order to allow implementation of the proposed principles?
3. How can the Bright ICT Indices be measured and their values converted to monetary terms in order to calculate the penalties, taxes, and tariffs globally?
4. What are the issues that need international agreements among user countries of the Bright Internet? What are the appropriate structure and functions of BIGG Center for the global agreement and governance?
5. What is the impact of the principles on the creation of solutions and services to enable new business platforms on the Bright Internet? What types of current solutions and services will be replaced by the new platform?

These issues should be investigated with a multidisciplinary effort between technology, business, economics, policy, and international relations. The potential conflict among different disciplines implies that there are opportunities to investigate consistent solutions between technology and policy. If a technology cannot be implemented due to a hindering policy, it is an opportunity to amend the policy. If a policy cannot be implemented due to a lack of technologies, it is an opportunity for research and development of the necessary technologies. In this manner, the future can be pursued through making the technology and policy consistent.

Concluding Remarks

The potential problems caused by the negative side effects of the Internet have been identified, and four principles have been proposed that construct the protocol of the Bright Internet: origin responsibility, deliverer responsibility, rule-based digital search

warrants, and traceable anonymity. In order to design the goal-driven protocol guided by these principles, some necessary technologies, policies, and international agreements have to be identified. Once the new platform of technology and policies that assures security and privacy is implemented, a variety of new business models will emerge.

Because the idea of the Bright Internet will solve many cyber security problems at a foundational level, the pursuit of goal seeking will create significant research potential. This approach enables IS research to be creative, futuristic, and design-oriented. The test bed will generate the platform for future experimental studies through which the potential values of new technical solutions and the impact of new policies can be evaluated.

Based on this experimental platform, business researchers can design new business models even before the industry begins in practice. This is a rare opportunity for IS researchers to become pioneers of creating a future society ahead of industry. In this regard, the endeavor of the Bright Internet can be contrasted with the current research practices that test theories using historical data. This research will create a fundamental solution for the bright future society. This is the onset of a new movement to overcome the negative side effects of the Internet.

References

AIS. 2015. "Committees and Task Forces: The Task Force on Bright ICT Initiative," http://aisnet.org/?CommitteesTaskForces.

Baba, T., and Matsuda, S. 2002. "Tracing Network Attacks to Their Sources," *IEEE Internet Computing* (6:2), pp. 20-26.

Blue Coat. 2014. "Press Release: Blue Coat Reveals Security Risks From 'One-Day Wonders' Websites," Blue Coat Systems Inc., August 26 (https://www.bluecoat.com/company/press-releases/blue-coat-reveals-security-risks-one-day-wonders-websites).

Cobb, C. 2003. *Network Security for Dummies*, Indianapolis, IN: Wiley Publishing, Inc.

Craig, T., and Ludloff, M. E. 2011. *Privacy and Big Data*, Sebastapol, CA: O'Reilly Media, Inc.

Deibert, R. 2013. *Black Code: Surveillance, Privacy, and the Dark Side of the Internet,* Toronto: McClelland & Stewart/Random House of Canada.

Deibert, R., Palfrey J., Rohozinski, R. and Zittrain, J. 2010. *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, Cambridge, MA: MIT Press.

eMarketer. 2014. "2 Billion Consumers Worldwide to Get Smart(phones) by 2016," December 11, http://www.emarketer.com/Article/2-Billion-Consumers-Worldwide-Smartphones-by-2016/1011694#sthash.nwYYS3BI.dpuf.

ERP. 2015. "European Recycling Platform," http://erp-recycling.org/who-we-are/profile.

Farrow, R. 2011. "Interview with Stefan Savage: On the Spam Payment Trail," *;login* (36:4), pp. 7-20 (http://cseweb.ucsd.edu/~savage/papers/LoginInterview11.pdf).

Greenwald, G. 2014. *No Place to Hide*, New York: Metropolitan Books.

He, S., Lee, G. M., and Whinston, A. B. 2014. "Estimating the Treatment Effect of Spam Information Disclosure on Organizations: A Field Experiment," in *Proceedings of INFORMS Conference on Information Systems Technology*, San Francisco, November 8-9.

Internet Live Stats. 2015. "Internet Users in the World," April 15, http://www.internetlivestats.com/total-number-of-websites.

Kohavi, L. 2014. "Internet Threats Trend Report," CYREN, Inc., October (http://www.cyren.com/tl_files/downloads/CYREN_Q3_2014_Trend_Report.pdf).

Lee, C., and Knight, D. 2005. "Realization of the Next-Generation Network," *IEEE Communications Magazine* (43:10), pp. 34-41.

Levmore, S., and Nussbaum, M. C. (Eds.). 2010. *The Offensive Internet: Speech, Privacy, and Reputation*, Cambridge, MA: Harvard University Press.

Neustar. 2014. *The Danger Deepens: The Neustar Annual DDos Attack and Impact Report*, Neustar, Inc., Sterling, VA (https://www.neustar.biz/resources/whitepapers/ddos-protection/2014-annual-ddos-attacks-and-impact-report.pdf).

Nissenbaum, H. 2010. *Privacy in Context: Technology, Policy and the Integrity of Social Life*, Stanford, CA: Stanford University Press.

Rao, J. M., and Reiley, D. H. 2012. "The Economics of Spam," *The Journal of Economic Perspectives* (26:3), pp. 87-110.

Savov, V. 2014. "Sony Pictures Hacked: the Full story," *The Verge*, December 8 (http://www.theverge.com/2014/12/8/7352581/sony-pictures-hacked-storystream).

Shao, M. 2009. "The European Recycling Platform: Promoting Competition in E-Waste Recycling," Stanford Graduate School of Business Case GS-67, Stanford University.

Singer, P., and Frideman, A. 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know,* Oxford, UK: Oxford University Press.

Solove, D. J. 2008. *Understanding Privacy*, Cambridge, MA: Harvard University Press.

Solove, D. 2011. *Nothing to Hide: The False Tradeoff Between Privacy and Security*, New Haven, CT: Yale University Press.

Sticca, F., and Sonja, P. 2013. "Is Cyberbullying Worse than Traditional Bullying? Examining the Differential Roles of Medium, Publicity, and Anonymity for the Perceived Severity of Bullying," *Journal of Youth and Adolescence* (42:5), pp. 739-750.

Stotz, A., and Sudit, M. 2007. "INformation Fusion Engine for Real-time Decision-Making (INFERD): A Perceptual System for Cyber Attack Tracking," in *Proceedings of the 10th IEEE International Conference on Information Fusion*, Quebec, July, pp. 1-8.

Symantec. 2013. "Norton Report," Symantec (http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013).

von Ahn, L., Bortz, A., Hopper, N. J., and O'Neil K. 2006. "Selectively Traceable Anonymity," in *Proceedings of the 6th Workshop on Privacy-Enhancing Technologies* (PET 2006, LNCS 4258), G. Danezis and P. Golle (eds.), Berlin: Springer-Verlag, pp. 208-222.

European Commission. 2015. "Waste Electrical & Electronic Equipment (WEEE)," March 27 (http://ec.europa.eu/environment/waste/weee/index_en.htm).

Yonhap News Agency. 2012. "Constitutional Court Rules Real-Name Policy Online Unconstitutional," *The Korea Herald,* August 23.

Wondracek, G., Holz, T., Kirda, E., and Kruegel, C. 2010. "A Practical Attack to De-anonymize Social Network Users," in *Proceedings of the 2010 IEEE Symposium on Security and Privacy*, Los Alamitos, CA: IEEE Computer Society Press, pp. 223-238.