Global Information Privacy Infringement Index (GPI)

Hyunmin Suh and Myungchul Kim
School of Computing
Korea Advanced Institute of Science and Technology
Daejeon, Republic of Korea
e-mail: {hyunmin088, mck}@kaist.ac.kr

***Abstract* - The proliferation of the Internet has attracted much attention with regard to the leakage of online private/personal information, as exposed information is being used for criminal purposes. In this regard, a criterion for information privacy must be clarified for governments and other public institutions as well as private enterprises in order to curtail information privacy violations and criminal activity. In order to apply such an information privacy criterion, we propose a global-scale information privacy infringement index, known as the Global Information Privacy Infringement Index (GPI). The GPI examines the level of information privacy infringement by measuring the factors, such as types, records, sources, characteristics, and actions based on infringed records for each country. Our approach can be a useful guide for governments, the public and private enterprises in their efforts to enhance information privacy.**

Keywords-information privacy; information privacy infringement; index.

I. INTRODUCTION

The number of Internet users stands at nearly 3.4 billion as of July, 2016, meaning that 40 percent of the world population is currently connected to the Internet [1]. The emergence of the Internet of Things (IoT) has also contributed to the rapid proliferation of mobile Internet users such that the Internet has now become absolutely inseparable tool from the lives of people.

Despite the great benevolent intention of the Internet, the leakage of online private/personal information has been a significant issue around the world. The security burden of protecting personal information applies to all countries. Currently, companies in the US are experiencing losses of more than 525 million US dollars annually due to cybercrime based on malicious codes [2]. The increase in cybercrime has had profound effects on consumers. The largest infringes of information amount to more than 130 million user accounts. The potential targets of phishing attacks are mostly online brands such as PayPal and EBay, an online payment provider and online auction site, respectively [2].

The importance of maintaining reasonable expectations of privacy does not literally mean only preserving personal information, but also, the respecting human rights. For instance, the Identity Card Act [3] was proposed in the UK in 2006. The Identity Card Act was proposed to facilitate a reliable and secure record of individual registrations in the UK. It also promises a useful means for individuals to prove their identities. Initially, it was created to protect Britain against terrorism, organized crime, and to prevent identity theft, illegal immigration and illegal employment. However, the Identity Card Act was repealed due to criticism related to privacy and human rights issues. Privacy campaigner, who stood against the Act, argued that the identity database is a likely target for abuse. For instance, members of the witness protection program, celebrities and victims of domestic violence can be targeted as vulnerable groups in that their personal information can be stolen and sold. Moreover, on 2 February 2005, the UK Parliament's Joint Committee on Human Rights challenged the compatibility of the Bill in consideration of Article 8 of the European Convention on Human Rights and Article 14, both from the Human Rights Act 1998 [4]. Thus, many in Britain believed that Identity Cards Act was in violation of the right to privacy and the right to non-discrimination, as encompassed in the Human Rights Act.

In South Korea, three major credit card companies were targeted by malicious outsiders, leading to the leakage of 104 million instances of information, specifically cardholders' personal and financial information, in 2013 [5]. After this major leak from the card companies, billions stolen from NongHyup Bank, one of the major banks in South Korea, it was assumed that hackers used pharming attack with the victims' personal information [6]. According to Statistics Korea (KOSTAT), 152,151 records were reported as undergoing an information privacy infringement in 2015. These instances are classified into unauthorized collections of personal information, unauthorized abuses of personal information, illegal uses of personal identification numbers, cases not subject to the law, and others. In the records, the illegal use of personal identification numbers accounts for the largest proportion of information privacy infringements, at 77,598 records, i.e., 51 percent of the entire number of records [7].

ISBN: 978-1-61208-605-7

Therefore, it is essential to make the conditions of the online environment safer and more secure by encouraging the involvement of the public and of the government. In this regard, a criterion pertaining to information privacy must be clarified by the government, public and private enterprises in order to curtail online privacy violations and criminal activity. In order to apply a criterion of privacy, we propose an information privacy index, which works on a global scale, known as the GPI. The GPI examines the level of information privacy by measuring the factors such as types, records, sources, characteristics, and actions based on infringed records which have occurred in the country. This approach can be a useful guide to the public and to government and private organizations as they attempt to enhance information privacy.

The contributions of this paper are as follows:

First, we propose the GPI as a means of measuring the level of information privacy for each country. With regard to the GPI, we successfully quantified the level of information privacy, making it much easier for people to increase their self-awareness of information privacy in their country of residence.

Second, we attempt to provide an empirical analysis on the basis of publicly available data. In this way, we do not provide any ambiguous or estimated data about the privacy level in near future but rather give information about the present based on the publicly disclosed records.

Last, we demonstrate the GPI for five countries as case studies by applying our method using infringed records from around the globe.

This paper is organized as follows. Section II consists of the basic concepts of the GPI. In this section, we clarify the definition and provide background information. Related work with regard to the GPI is presented in Section III. In Section IV, a description of GPI is given in detail. The GPI is measured and evaluated in Section V. We finalize the paper in Section VI.

II. Basic Concepts

This section presents the definition of privacy and information privacy and background information related to GPI.

A. Privacy, Information Privacy and Personal Information

Privacy is ambiguous in that includes a broad range of concepts, such as freedom of thought, control over personal information, and others. According to the United Nation (UN), “Privacy can be defined as the presumption that individuals should have an area of autonomous development, interaction and liberty, a ‘private sphere’ with or without interaction with others, free from State intervention and from excessive unsolicited intervention by other uninvited individuals. The right to privacy is also the ability of individuals to determine who holds information about them and how that information is used” [8].

Privacy has become a controversial issue which has a profound impact around the globe. Protecting privacy is now a subjective goal for nearly every nation, with numerous statutes, constitutional rights, and judicial decisions affecting these efforts. Most nations around the globe note privacy in their constitutions for the protection of citizens. Even if privacy is not mentioned in constitutions, many countries are aware of the importance of constitutional rights to privacy, including Canada, France, Germany, Japan, and India [9].

Information privacy is an emerging topic with the advent of the Internet, as personal information is digitalized on the Internet for many purposes. The definition of information privacy must encompass an important feature to refer also to the privacy of digitalized personal data which is stored on a computer system. Information privacy concerns the collection and dissemination of data, technology, legal and political issues surrounding them.

There is great ambiguity in the way ‘personal information’ is used. In the context of privacy or academic research, personal information refers to information that is sensitive and any information that can designate or identify a person [10]. Personal information, under the law of South Korea, is defined as a personal information related to a natural person whom he or she must be alive. Personal information means an information that can designate or identify an alive person. If collected information does not identify a person, it still counts as a personal information when collected information can be easily combined with other information [11]. In the European Union Directive, “personal data shall mean any information relating to an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity [12].” Personal information can appear in online and offline environments. This paper focuses on digitalized personal information that is acquired, stored on, abused, and/or removed from a computer system.

B. Personal Identification Number

The definition of a ‘personal identification number’ [13] differs for each country. Such numbers are termed national identification number, national identity number, national insurance number, personal identification number, or resident registration number. The governments of many countries use personal identification number as means of tracking citizens and permanent/temporary residents. Personal identification numbers can be given to foreigners for guidance and to differentiate them from citizens. Moreover, personal identification numbers can be used for tracking for the purposes of employment, taxation, governmental benefits, health care, and other government related functions. They are not widely used in relation to violations of human rights, but some countries still maintain the system for convenience in managing citizens.

Various personal identification number systems are implemented among countries; however, most nations issue an identification number when citizens are born or when they reach a certain age (or legal age). For noncitizens, identification numbers can be issued when they enter the country and/or when they are granted a temporary/permanent resident permit, but the numbers will be issued with a different logic from that used with citizens. Many countries have attempted to issue identification numbers for singular purposes, but many of these efforts have been halted due to strong resistance from human rights movements. In fact, personal identification number system is still used in some countries.

C. *A Comparison of Personal Identification Number Systems*

As noted above, personal identification number systems vary across among countries. In this subsection, we provide more detailed information about the personal identification number among five countries; the United States, the United Kingdom, Germany, Japan, and South Korea. In addition, we analyze the domain of personal identification number in five sector; Passport Issuance, Driver License, Taxation, Social Insurance, and Finance summarized in Table 1. These five sectors are critical in that each nation uses a different approach to authenticate users and collect personal information.

The United States developed its Social Security Number (SSN) [14] system for the organization of social security related benefits. However, the number is now used for other purposes, working as a personal identification number system. For passport issuance, a person needs to prove his or her citizenship (such as proof of birth, certification of citizenship, or certification of naturalization), and the SSN must be given [15]. For a driver's license, proof of birth and identification documents must be given along with the SSN [16]. For taxation, four types of taxation numbers exist; Taxpayer Identification Number (TIN), Employer Identification Number (EIN), Individual Taxpayer Identification Number (ITIN), and Preparer Taxpayer Identification Number (PTIN) [17]. For finance, the SSN is not necessarily a required condition.

In the United Kingdom, there is no official personal identification number system and legal requirement to possess any types of identification document to prove one's identity. However, there is the National Insurance Number (NIN) [18], which is issued to all citizens in the United Kingdom for the purpose of insurance. The NIN is issued when legal age is turned 16. The NIN is not mandatory to possess, and driver's license is generally used as proof of identity. In order to issue a driver's license, proof of identification must be submitted such as proof of birth or a passport. When applying online, the driver's license issuing institution may collect the NIN [19]. For taxation, the NIN is needed in order to issue a Unique Tax Reference (UTR). Employers collect the NINs of employees for taxation related purposes [20]. For finance, the NIN is rarely used, whereas driver's licenses and passports are mostly used as proof of address and identity [21].

In Germany, there is the Neuer Personalausweis (nPA), but it does not function as a personal identification number. The nPA, which is known as an ID card system, is heavily regulated in terms of its usage. Almost every sector issues a unique number that each sector such as passport, driver license, taxation, social insurance, and finance has its own unique number. The nPA is used as an authentication method but storing or wiring nPA information with the unique number is regulated. This ID card system nPA is implemented in 2010 that is an electronic high-tech ID card using, for instance, Radio-Frequency ID (RFID), cryptographic technique, secure storage, and others. Validation using the nPA lasts 10 years, and a new number is issued when the card is lost or reissued. The collection of the nPA by private institution is illegal. For the protection of personal information, there is no unified number that grants access to social security services in Germany. There are unique numbers for each social security services wiring these numbers with the nPA is illegal [22][23].

My Number [24] of Japan is a newly emerging personal identification number system which started in 2016. My Number is a 12 digits number issued to all residents of Japan, including temporary and permanent residents with valid permits. The previous personal identification number system was only used for taxation, social insurance, and medical insurance purposes. However, the Japanese government has stepped forward to centralize the system with a number for nearly every sector, to eventually become a unique number for the entire system. Thus, My Number will be used for taxation, social security, driver's license, and a passport [25].

In South Korea, the Resident Registration Number (RRN) [26] is a 13-digit number issued to all residents of the country. The system started on November of 1968 for the purpose of identifying spies. The RRN is used in nearly every sector not only as an authentication method but also as a key number with which to make inquiries into the system. Even up to August of 2012, the RRN was ruthlessly collected by public and private institutions for convenience [27]. There are critical problems which have long occurred in South Korea associated with the extensive use of the RRN. First, the South Korean government has implemented an e-government system and there are at least 1,100 information systems under 47 administrative agencies which are linked in a single integrated government network [28]. These distributed information systems are integrated instantly when the RRN is entered into the system. Thus, personal information in every sector can be easily acquired by the government which can lead to the serious problem of state surveillance. Secondly, the meaningless collection of the RRN by private companies has led to many accidents, such as leakages of RRN. Moreover, the most critical problem related to the RRN is that leaked RRNs cannot be changed during the course of one's lifetime once they are issued.

TABLE I. A COMPARISON OF PERSONAL IDENTIFICATION NUMBER SYSTEMS

	Taxation	Passport	Driver's License	Social Insurance	Finance	Change of Personal Identification Number
U.S (SSN)	Δ	O	O	O	Δ	Cannot be changed (except in cases of error)
U.K (NIN)	O	X	X	O	X	Cannot be changed
Germany (nPA)	X	X	X	X	X	Changed in every 10 years
Japan (My Number)	O	O	O	O	X	Cannot be changed
South Korea (RRN)	O	O	O	O	O	Cannot be changed

* O: Must, Δ: Optional, X: Not required

III. RELATED WORKS

In this section, we briefly survey the works that are relevant to the GPI.

A. The Breach Level Index

The Breach Level Index [29] aims to provide the overall breach severity level by tracking publicly known breaches to allow organizations to measure their own risk assessment. The Breach Level Index does not set an upper limit, but the largest breach scores are 10 thus far. The Index is in logarithmic (base 10) scales used similar to the scales for volcanoes and earthquakes [30][31]. However, the Breach Level Index is designed to provide a risk assessment tool specifically targeting enterprises. The GPI tends to complement the weaknesses of the Breach Level Index to provide a national level scale to acknowledge the level of information privacy infringement.

B. The Global Cybersecurity Index

The Global Cybersecurity Index [32] is a project that aims to measure each nation's level of commitment to cybersecurity. The final goal of the GCI is to advocate for a global culture of cybersecurity and its integration in terms of information and communication technologies. The Global Cybersecurity Index covers the five areas of legal measures, technical measures, organizational measures, capacity building, and cooperation. These five areas have a profound impact on cybersecurity with regard to assessing national capabilities as they form the building blocks of national capabilities. The GCI covers various fields but their global ranking of cybersecurity index is relatively impractical. The GCI only focuses on the existence of national structures in place rather than actual cybersecurity level for a particular country. Ironically, the GCI has reported that the United States of America is placed at first in their cybersecurity index; however, the U.S. is happened to be the country with highest number of cybersecurity related accidents according to the Breach Level Index. GPI scale aims to provide information based on infringed records that focuses more on evidence rather than the infrastructure. Thus, GPI is based on the fact itself as well as the details occurred in the specific country.

C. The Global Conflict Risk Index

The Global Conflict Risk Index (GCRI) [33] was developed by the Joint Research Center. The GCRI is designed to assist with decision making about long-term conflict risk by providing accessible and objective open sources. The contributions of the GCRI are described as follow: It clarifies the definitions of 'risk' and 'risk conflict' which derived from existing methodologies of conflict research. In addition, five risk areas for each state are presented for a quick overview of the structural conditions of the state. Moreover, it provides an evaluation and an assessment of a particular country's risk. The GCRI is focused on the risk that can occur in a certain country. However, the GPI is more focused on infringement level as opposed to the level of risk in a country.

D. The Crime Rate

The crime rate represents the number of offenses per certain number of people. The Federal Bureau of Investigation (FBI) [34] releases crime statistics, dividing the number of crimes by 100,000 inhabitants. The GPI has benchmarked the concept of the crime rate as the number of infringed records per the number of data production. Moreover, we attempt to provide a level of information privacy infringement at present based on the publicly disclosed records.

IV. THE DESCRIPTION OF THE GPI

This section presents a description of the GPI with regard to categories and methodology.

A. *Categories*

The GPI model deals with five factors, as seen in Table 2. 'N' represents the total number of infringement records, specifically representing when private information has been leaked. For instance, the number of records infringed was 24 million in the case of Zappos, when they were hacked by a malicious hacker [35]. We measure the total IP traffic of the country as 'I', as indicated. Since the amount of data production is not publicly available, the total IP traffic brought by Cisco VNI [36] is used to consider the amount of data produced in a certain country. The type of data in the records 't' ranging from 1 (least) to 5 (most) covering all types of data, ranging from less important information to the most important information. Identity theft, which is ranked 4 in Table 2, has been developed from the conventional type specifically noting what types of identification were infringed. It is important to consider what caused the information to be leaked. In this regard, 's' represents the source of the infringement ranging from 1 to 5 and covering a lost/stolen device, malicious insider/outsider, and state sponsored attacker. Leaked information can be replaced or reissued but particular information is an exception. For example, if a user's email address is leaked, it can be easily replaced with another email address. The user may experience inconvenience when replacing his lifelong email address but it may not harm his personal life. However, an information like RRN, a type of personal identification number in South Korea, is permanent and unique number and being used for multiple purposes as a method of online/offline authentication. As a consequence, leaked RRN has been adversely abused for pharming attack, phishing, and various types of fraud. In this sense, it is vital to measure the value of personal identification number system as noted 'c' as characteristics of personal identification number system in the GPI. The 'c' is ranging from 1 to 5 with regard to the personal identification number system. Leaked information can be used for the secondary purposes as well. Stolen identity can be used to target the victim, or it can be used to access their financial account. The type of actions denoted by 'A' in the GPI refers to instances of the secondary use of data.

TABLE II. CATEGORIES OF THE GPI

N = the total number of infringement records	
I = Total IP traffic information according to the Cisco Visual Networking Index (Cisco VNI), an ongoing initiative to track and forecast the impact of visual networking applications	
t = the type of data in the records	
values	
1	Email addresses
2	Online account access (username/passwords to social media, websites, etc.)
3	Financial access (bank account credentials, credit card data)
4	Identity theft (such as personal identification Number, driver's license number, etc.)
5	Confidential information (highly sensitive information on a national scale)
s = source of the infringement	
values	
1	Lost device (such as a laptop, OTP or USB)
2	Stolen device
3	Malicious insider
4	Malicious outsider
5	State sponsored
c = characteristic	
values	
1	Lost personal identification number can be replaced, reissued or recovered easily, and no harm done
2	Lost personal identification number can be replaced, reissued or recovered, it may be used for humiliation, but not financially damaging
3	Lost personal identification number can be replaced, reissued or recovered, but it may be used for secondary purposes
4	Lost personal identification number cannot be replaced, reissued or recovered, and it can be used to gain financial access
5	Lost personal identification number cannot be replaced, reissued or recreated, and it can cause serious damage or be used for secondary purposes
A = whether secondary actions are taken (for criminal or humiliation purposes)	
values	
1	No action
2	Publication of embarrassing information or used for humiliation
3	Publication of harmful information such as hacker logs, etc.
4	Access to financial websites or private websites
5	Use of financial identity to obtain financial funds or any damage to finances

B. *Methodology*

The methodology of our approach for the GPI relies on publicly disclosed infringed records. The equation of the GPI is presented below.

$$\text{GPI} = \sum_{x=1}^{n}[\log(\frac{N}{I} * t * s * c * A)]_x$$

The GPI aims to cover all infringed or leaked information occurring at a national level. We divide the total number of infringement records 'N' by 'I' denoting the IP traffic of a country. After multiplying each category of the data, we use the logarithm (base 10) scale to make it as simple as the system used in the Breach Level Index. In the equation, 'x' represents an event of each infringed record which occurs in a particular country. The sum of 'n' number of records will represent the entire set of infringed information occurring in a certain country. Finally, the score of the GPI does not set the upper limit as benchmarked from the crime rate.

V. EVALUATION

We evaluate the GPI based on the methodology introduced in the previous section. We used the sets of infringed records derived from Breach Level Index [29] for five countries such as the United States, the United

Kingdom, Japan, Germany, and South Korea and obtained their privacy levels.

TABLE III. RESULT OF THE GPI

Country	Contents		
	Infringed Records (2014)	***GPI***	***Rank***
United States	1,257	933.7	1
United Kingdom	135	159.4	2
South Korea	12	73.4	3
Japan	12	30.7	4
Germany	10	14.1	5

Among many other countries, the United States accounts for the largest amount of infringed information around the world. There are 1,257 infringed records for the period from January 1st, 2014 to December 31st, 2014. However, due to the exceeding number of records, we discard the records scoring below 6 in the Breach level Index. The data of the United States implies that more information infringements are likely to occur in the United States, as much more information is produced there than in any other country. The total amount of IP traffic produced within the United States was 18.1 exabytes in 2014, clearly higher than those figures for other countries. As a result, the United States scored 934 on the GPI. Various causes can explain why the United States is the country with the greatest amount of infringed information, but this does not mean that the level of privacy is low there. It is arguable that the United States may report the infringement records more transparently than other countries.

Similar to the United States, the total number of infringed records was 135 in 2014 in the UK. We discarded information which scored under 6 points from the dataset for the same reason given in the previous case. We accumulated all of the infringed record of the United Kingdom in 2014 as well as the total IP traffic in 2014, which was 2.4 exabytes. The United Kingdom does not have a personal identification number, with individual identification numbers issued from different institutions. In this sense, most of the identification numbers in the UK can be replaced or reissued easily, but information there can still be used to identify a person. As a result, the United Kingdom scored 159 on the GPI.

In South Korea, there are 12 infringed records in 2014. Although South Korea has fewer infringed records, they scored 73. In 2014, the three largest credit companies had 104 million records of personal information stolen and leaked, including RRN. Unlike other countries, South Korea is the only country using a RRN, a personal identification number system for which the number cannot be replaced or reissued once it is issued. The RRN can be used as an online and offline as a means of authentication, and it is used extensively in many sectors in South Korea. Most phishing and pharming attacks are initiated by identifying a person through their RRN. Thus, the RRN is a critical factor which violates the privacy level in South Korea, and this resulted in a higher GPI score.

In Germany, there are ten infringed records in 2014. Compared to the United States and the United Kingdom, there are relatively few records. Germany's GPI is 38. Germany has a strong regulation on the usage of personal identification number system that the domain of ID card is far lower than any other countries. The nPA, an ID card system of Germany, can easily be replaced and reissued that it has absolutely no harm on citizens in Germany.

In Japan, since there are 12 infringed records in 2014, the GPI is 31. The GPI score is low, but several factors should be considered. Japan has adopted an electronic national identification number system known as 'My Number' that can be used to identify a person. The system can lead to serious phishing or pharming attacks, as shown in the case of South Korea. However, the infringed information in 2014 does not include any information from the 'My Number' system, resulting in a score for Japan that was relatively low compared to those of other countries.

VI. CONCLUSION AND FURTHER WORK

The GPI aims to provide a useful criterion when dealing with information privacy infringement issues on a global scale. The GPI can be enhanced in various forms, such as through a regression analysis, a multi-year data analysis, and others. The model can be advanced if we consider the cost aspects of information privacy infringement. Moreover, multi-year data of the cost is publicly disclosed, our model can be much developed.

Our initiative of providing information about the level of information privacy infringement on a global scale is certainly a valuable means of alerting to the world. We continue to complement our GPI methodology to cover every country around the world for a brighter and more secure future.

ACKNOWLEDGEMENT

This work was supported by a grant from the National Research Foundation of Korea (NRF) funded by the Korean government (MSIP) (No. 2017R1A2B4005865).

REFERENCES

[1] Internet Live Stats., [Online]. Available from: http://www.internetlivestats.com/internet-users/ [Last access: March, 2016]

[2] Statista., "Statistics and Market Data on Cyber Crime" [Online]. Available from: http://www.statista.com/markets/424/topic/1065/cyber-crime/ [Last access: March 2016]

[3] The Guardian., [Online]. Available from: http://www.theguardian.com/commentisfree/libertycentral/2009/jan/15/identity-cards-act [Last access: March, 2016]

[4] European Commision. "UK's ID Cards Bill wins parliamentary vote despite Human Rights concerns" [Online]. Available from: http://ec.europa.eu/idabc/servlets/Docee17.pdf?id=21693 [Last access: March, 2016]

[5] Joongangdaily., [Online]. Available from: http://koreajoongangdaily.joins.com/news/article/article.aspx?aid=2983762 [Last access: March, 2016]

[6] Koreabang., [Online]. Available from: http://www.koreabang.com/2014/stories/hackers-steal-billions-from-nonghyup-bank-is-not-responsible.html [Last access: March, 2016]

[7] Statistics Korea., [Online]. Available from: http://www.index.go.kr/potal/main/EachDtlPageDetail.do?idx_cd=1366 [Last access: March, 2016]

[8] Techopedia., "Information Privacy." [Online]. Available from: https://www.techopedia.com/definition/10380/information-privacy [Last access: April, 2016]

[9] D., Solove, "Understanding Privacy," Harvard University Press, 2008.

[10] H., Nissenbaum, "Privacy in Context: Technology, Policy, and the Integrity of Social Life," Stanford University Press, 2010.

[11] Ministry of Interior., "Persoanl Information Protection Act, Article 2," [Online]. Available from: https://www.privacy.go.kr/eng/laws_policies_list.do [Last access: April, 2016]

[12] Data Protection Commissioner (DPC), "EU Directive 95/46/EC – The Data Protection Directive, Chapter 1 – General Provision," 2016.

[13] Record Union., "What is a national identification number?," [Online]. Available from: http://helpdesk.recordunion.com/FAQ/what-is-a-national-identification-number [Last access: April, 2016]

[14] Social Security., "The Story of the Social Security Number," [Online]. Available from: https://www.ssa.gov/policy/docs/ssb/v69n2/v69n2p55.html [Last access: April, 2016]

[15] U.S. Passports & International Travel, "First Time Applicants," 2016 [Online]. Available from: https://travel.state.gov/content/passports/en/passports/first-time.html [Last access: April, 2016]

[16] California Department of Motor Vehicles. "Social Security Number (FFDL 8)," 2016 [Online]. Available from: https://www.dmv.ca.gov/portal/dmv/detail/pubs/brochures/fast_facts/ffdl08 [Last access: April, 2016]

[17] Internal Revenue Service, "Taxpayer Identification Number (TIN)," 2016 [Online]. Available from: https://www.irs.gov/individuals/international-taxpayers/taxpayer-identification-numbers-tin [Last access: May, 2016]

[18] UK Government, "National Insurance," [Online]. Available from: https://www.gov.uk/national-insurance/your-national-insurance-number [Last access: May, 2016]

[19] UK Government, "Apply for your first provisional driving license," 2016 [Online]. Available from: https://www.gov.uk/apply-first-provisional-driving-licence [Last access: May, 2016]

[20] Unique Taxpayer Reference Government, "How to get u UTR Number if Self Employed," [Online]. Available from: http://utr.org.uk/home [Last access: May, 2016]

[21] Barclays, "Identification for bank accounts," 2016 [Online]. Available from: http://www.barclays.co.uk/validid [Last access: May, 2016]

[22] German-way.com, "The Identity Card –der Ausweis," [Online]. Available from: http://www.german-way.com/for-expats/living-in-germany/the-identity-card-der-ausweis/ [Last access: May, 2016]

[23] M., Margraf, "The New German ID Card," [Online]. Available from: http://www.personalausweisportal.de/SharedDocs/Downloads/EN/Paper_new_German_ID-card.pdf?__blob=publicationFile

[24] Cabinet Secretariat, [Online]. Available from: http://www. gov-online.go.jp/tokusyu/mynumber/ad/?sec1_kojin_2-2 [Last access: May, 2016]

[25] M., King, "My Number system: a worring glimpse of the future," 2015 [Online]. Available from: http://www.japantoday.com/category/opinions/view/my-number-system-a-worrying-glimpse-of-the-future [Last access: May, 2016]

[26] OECD, "Information on Tax Identification Numbers Section," [Online]. Available from: https://search.oecd.org/tax/automaticexchange/tinsandtaxresidency/taxidentificationnumberstins/Korea-TIN.pdf [Last access: May, 2016]

[27] Koreabang, "Korean Government Reorganizes National ID System After Leaks," 2014 [Online]. Available from: http://www.koreabang.com/2014/stories/korean-government-reorganizes-resident-registration-number-system.html [Last access: May, 2016]

[28] Ministry of Public Administration and Security, "e-Government in South Korea" [Online]. Available from: http://unpan1.un.org/intradoc/groups/public/documents/UNGC/UNPAN043625.pdf [Last access: May, 2016]

[29] BreachlevelIndex.com, [Online]. Available from: http://breachlevelindex.com/#!breach-database [Last access: May, 2016]

[30] S., Huler, "Defining the Wind: The Beaufort Scale and How a 19th-Century Admiral Turned into Poetry," 2014.

[31] Melaragno, M., "Severe Storm Engineering for Structural Design, " 1996.

[32] The Global Cybersecurity Index, [Online]. Available from: http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx [Last access: May, 2016]

[33] The Global Conflict Risk Index, "The Global Conflict Risk Index (GCRI) a Quantitative Model," 2014.

[34] FBI., "FBI Releases 2014 Crime Statistics" [Online]. Available from: https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-2014-crime-statistics [Last access: May, 2016]

[35] CNN Money., "Zappos hacked, 24 million accounts accessed" [Online]. Available from: http://money.cnn.com/2012/01/16/technology/zappos_hack/ [Last access: May, 2016]

[36] Cisco.com., "The Zettabyte Era – trends and Analysis" [Online]. Available from: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.html [Last access: May, 2016]

ISBN: 978-1-61208-605-7