https://doi.org/10.48009/1_iis_2015_7-14

Issues in Information Systems
Volume 16, Issue I, pp. 7-14, 2015

FAIR INFORMATION PRACTICES AT THE FORTUNE 500: AN EXAMINATION BY ORGANIZATION SIZE AND INDUSTRY SECTOR

Carl J. Case, St. Bonaventure University, ccase@sbu.edu
Darwin L. King, St. Bonaventure University, dking@sbu.edu

ABSTRACT

The unprecedented level of recent online corporate data breaches has caused consumer confidence to be shaken. As a result, this study was undertaken to comprehensively examine the privacy policies designed to protect the stakeholders of the largest firms, the Fortune 500. A content analysis of policies indicates that although nearly all firms have a policy posted on their website, the fair information practice principles of notice/awareness, choice/consent, access/participation, and security/integrity are not equally applied and vary by firm size and by industry sector. Results suggest that firms may be at risk and a more proactive approach should be taken with regard to policies.

Keywords: Fair Information Practices, Privacy, Fortune 500, Industry Sector

INTRODUCTION

Online data breaches are reaching unprecedented levels in scope and cost. In 2014 alone, Sony Corporation was reportedly hacked by North Korea, a data breach at JP Morgan Chase and Company affected 80 million U.S. households and 7 million small to medium-sized businesses, nude photos of Hollywood celebrities were extracted from iCloud accounts and posted online, 13 gigabytes of Shapchat data were pilfered, 56 million credit card numbers and 53 million email addresses were leaked by Home Depot, and eBay claimed a $200 million loss as a result of 145 million of its users being affected by hacking [15]. The Kroll 2013/2014 Global Fraud Report survey of 901 senior executives worldwide found that information theft was the second most common fraud (22% of companies) after theft of physical assets (28% of companies) [6]. Moreover, information theft was listed as the most highly vulnerable type of fraud by 21% of companies, an increase from 7% of companies in the prior year.

As a result, there has been a loss of consumer confidence. An Associated Press-GfK interview of 1,060 U.S. adults, for example, found that 58% have deep worries when spending online and 62% percent are very concerned when they buy on their mobile phones [5]. Eighty-eight percent of respondents place the burden on the retailers that collect personal data. In fact, a *USA TODAY* poll of 790 Internet users found that 24% of those surveyed indicated that they stopped purchasing online in recent weeks because they were concerned about the safety of information they might put online [14]. Another 56% indicated cutting back on the number of Internet sites they used and were only accessing large, well-known companies they were confident were safe. A demographic analysis shows that 30% of individuals who have not attended college had stopped buying online compared to 16% of those with college degrees. Of individuals with incomes under $30,000, 34% had stopped buying online compared to 15% of those with income of $75,000 or more. Interestingly, 64% of those surveyed indicated that they had changed a password in response to security breaches.

Businesses, on the other hand, have optimistic outlooks but troubling practices with regard to data security. A survey of 1,015 U.S. small and medium-sized businesses by the National Cyber Security Alliance and Symantec found, for instance, that 77% stated their company is safe from cyber threats such as hackers, viruses, malware or a cybersecurity breach, yet 83% percent have no formal cybersecurity plan [12]. Seventy-three percent stated that a safe and trusted Internet is critical to their success and 77% indicated that a strong cybersecurity and online safety posture is good for their company's brand. However, 59% do not have a contingency plan outlining procedures for responding and reporting data breach losses. Sixty-six percent are not concerned about cyber threats – either external or internal. External threats include a hacker or cyber-criminal stealing data while internal threats include an employee, ex-employee, or contractor/consultant stealing data. Eighty-six percent indicated that they are satisfied with the amount of security they provide to protect customer or employee data and 83% percent strongly or somewhat agree that they are doing enough or making enough investments to protect customer data.

The 2013 Small Business Technology Survey of 845 small business owners conducted by the National Small Business Association found 82% have a traditional website and 18% have a mobile website [4]. Although 59% indicated that cybersecurity is very important to the business, 27% had a low or no understanding of the online security issues and only 14% perceived that security issues are a challenge with regard to their website. Moreover, 72% of the businesses handle the online security internally. In addition, while 40% collect customer information, only 64% obtain approval from customers before collecting, storing, using, or disclosing their personal data.

Unfortunately, the PriceWaterhouseCoopers' 11th cybercrime survey of 500 U.S. executives, security experts, and others from the public and private sectors found that only 22% of respondents conduct incident response planning with their third party supply chain [10]. Although 52% of organizations have a formalized plan outlining policies and procedures for reporting and responding to cybersecurity events committed against the organization, only half of these firms test them at least once per year.

Governments appear to be taking notice. In 2014, 23 U.S. states introduced or considered security breach notification legislation [9]. Overall, 47 states have a law requiring consumer notification of security breaches involving personal information.

Given this apparent dichotomy between business optimism and stakeholder concern/government reaction regarding breaches, this research was conducted to examine several questions. What is the state of online privacy at the largest corporations? Do the fair information practices vary by firm size? Is industry sector a factor with regard to policies? Results are important in helping business firms to better understand stakeholder data issues and to assist in identifying potential risks.

FAIR INFORMATION PRACTICES

Fair information practice (FIP) principles have been recognized by U.S. government agencies since 1974. These principles are based in part upon the right to privacy as described in the *Harvard Law Review* in 1890 by Louis Brandeis and Samuel Warren [13]. They defined protection of the private realm as the foundation of individual freedom in the modern age. In the U.S. today, the Federal Trade Commission (FTC) promotes adherence to the principles to insure effective privacy protection [8].

The four FIP principles are:

- Notice/awareness – consumers have the right to know if personal information is being collected and how it will be used. Thus, data collectors must disclose their information practices before collecting information from consumers;
- Choice/consent – consumers must be given options with respect to whether and how information collected from them may be used for purposes beyond those for which the information was provided;
- Access/participation – consumers should be able to view and contest the accuracy and completeness of data collected about them and to correct errors; and
- Security/integrity – data collectors must take reasonable steps to assure that information collected from consumers is secure from unauthorized use during transmission and storage.

The corporate policies regarding online collection, use, and dissemination of personal information are commonly posted on company websites. Although developing and posting a policy does not guarantee compliance, the absence of a policy violates "notice/awareness," one of the fundamental FIPs.

PREVIOUS RESEARCH

There have been two major previous research studies related to the online privacy policies of the *Fortune* 500. Each study examined the location of the policy and the inclusion of the FIP principles.

The first study was conducted in 2002 [8]. Results indicated that 52% of the *Fortune* 500 firms had a privacy policy posted on its website with the majority, 87%, of those firms using a link from the home page and 13% with policies located elsewhere on the website. An examination by industry classification found that more than three-quarters of

firms in the arts, entertainment, and recreation, information, and finance and insurance areas had privacy policies. In terms of FIP principles, 92% addressed notice/awareness, 27% addressed access/participation, less than half complied with choice/consent, and 46% described security/integrity. In addition, 26% addressed children protection.

Another study empirically investigated the information privacy policies in 2006 [11]. A content analysis found that 79% of the firms had a policy posted on its website with 86% of those firms using a link from the homepage and 14% with policies located elsewhere on the website. In terms of FIP principles, 98% addressed notice/awareness, 61% addressed choice/consent, 45% addressed access/participation, and 71% addressed security/integrity.

Because the composition of the *Fortune* 500 is constantly changing and the previous research studies are now dated, this study was conducted to examine the current state of policy adoption and composition. In addition, this study builds upon prior research by exploring organization size, industry sector, and additional practices and policies.

RESEARCH DESIGN

This study used the *Fortune* magazine website to obtain the *Fortune* 500 company directory and the corresponding company home page web address [3]. A two-step process was used to locate privacy policies for each organization in September of 2014 (Figure 1). First, each company home page was examined for privacy policy links. Next, if a privacy policy link was not found on the home page, the home page's search engine was utilized to search for the policies. A content analysis of the posted information privacy policies was then conducted to examine each firm's use of the FIP principles, additional policies, data collection procedures, and security techniques. Resultant data was analyzed by organization size and industry sector.

Figure 1. Research Methodology

RESULTS

A review of the *Fortune 500* firms found that 94% of these firms have a privacy policy posted on their website. In terms of location, 90% of the firms have the policy link located on the company home page and 4% have the policy located on another web page (Table 1).

Table 1. Privacy Policy Website Location

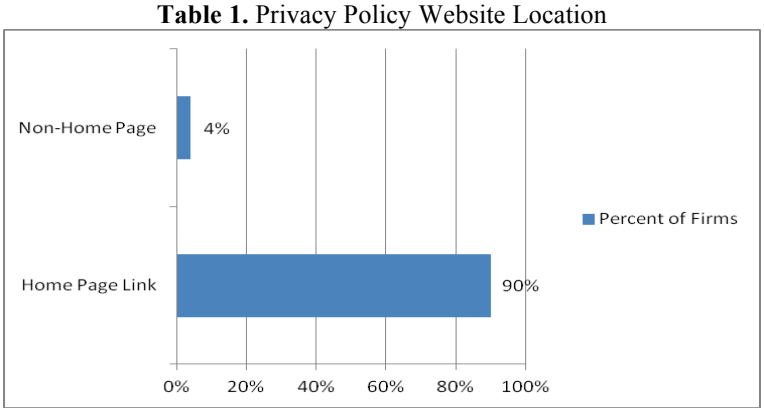

Table 3 provides a breakdown of privacy policy usage and policy composition by firm size. Privacy policies, for example, are implemented by 100% of the *Fortune* 1-100 firms, 93% of the *Fortune* 101-200 firms, 95% of the *Fortune* 201-300 firms, 91% of the *Fortune* 301-400 firms, and 91% of the *Fortune* 401-500 firms. When examining the *Fortune* 1-100, 95% of firms provide notice/awareness, 92% describe choice/consent, 70% discuss access/participation, and 64% address security/integrity. In terms of the *Fortune* 101-200, 89% of firms provide notice/awareness, 78% describe choice/consent, 64% discuss access/participation, and 67% address security/integrity. In terms of the *Fortune* 201-300, 96% of firms provide notice/awareness, 85% describe choice/consent, 70% discuss access/participation, and 80% address security/integrity. In terms of the *Fortune* 301-400, 88% of firms provide notice/awareness, 72% describe choice/consent, 58% discuss access/participation, and 71% address security/integrity. In terms of the *Fortune* 401-500, 86% of firms provide notice/awareness, 76% describe choice/consent, 65% discuss access/participation, and 69% address security/integrity. Overall, the *Fortune* 201-300 have the largest percentage of firms that implement 3 of the 4 policy principles, the exception being choice/consent, which has the highest usage in the *Fortune* 1-100 firms. In addition, the most implemented principles are notice/awareness and choice/consent while the least implemented principles are access/participation and security/integrity.

Table 2. Policy Usage and Composition By Firm Size

	Fortune 1-100	**Fortune 101-200**	**Fortune 201-300**	**Fortune 301-400**	**Fortune 401-500**
Privacy Policy	100%	93%	95%	91%	91%
Notice/Awareness	95%	89%	96%	88%	86%
Choice/Consent	92%	78%	85%	72%	76%
Access/Participation	70%	64%	70%	58%	65%
Security/Integrity	64%	67%	80%	71%	69%

Next, the usage of addition practices and principles by firm size was examined (Table 3). Cookies or beacons, tools for data collection, are described by 92% of the *Fortune* 1-100 firms, 78% of the *Fortune* 101-200 firms, 85% of the *Fortune* 201-300 firms, 72% of the *Fortune* 301-400 firms, and 76% of the *Fortune* 401-500 firms. Specifically, a cookie is a text file with tracking number that is downloaded onto a user's computer hard drive and a beacon is a transparent graphic (one pixel wide and one pixel deep) embedded in a web page or email and is used to report the visitor's IP address and cookie information [8].

SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are standard security technologies for establishing an encrypted link between a server and a client—typically a web server (website) and a browser [2]. When examining the *Fortune* 1-100, 24% of firms use SSL/TLS security, 44% describe mobile application policies, and 71% detail children policies. In terms of the *Fortune* 101-200, 23% of firms use SSL/TLS security, 26% describe mobile application policies, and 58% detail children policies. In terms of the *Fortune* 201-300, 25% of firms use SSL/TLS security, 32% describe mobile application policies, and 54% detail children policies. In terms of the *Fortune* 301-400, 20% of firms use SSL/TLS security, 19% describe mobile application policies, and 48% detail children policies. In terms of the *Fortune* 401-500, 17% of firms use SSL/TLS security, 28% describe mobile application policies, and 54% detail children policies. Overall, the *Fortune* 1-100 have the largest percentage of firms that implement 3 of the 4 additional practices and policies, the exception being SSL/TLS, which has a slightly larger usage in the *Fortune* 201-300 firms. In addition, the most implemented additional practices and policies are cookies/beacons and children policies while the least implemented additional practices and policies are SSL/TLS and mobile application policies.

Table 3. Additional Practices and Policies by Firm Size

Practice/Policy	Fortune 1-100	Fortune 101-200	Fortune 201-300	Fortune 301-400	Fortune 401-500
Cookies/Beacons	92%	78%	85%	72%	76%
SSL/TLS	24%	23%	25%	20%	17%
Mobile Application Policies	44%	26%	32%	19%	28%
Children Policies	71%	58%	54%	48%	54%

Table 4 provides an analysis of privacy policy usage and policy composition by industry sector. Industry sector was specified in the CNN Money website data. In an effort to simplify the analysis, only industry sectors with at least 10 firms within that sector were summated. This resulted in 16 industry sectors, accounting for 60% of the firms in the *Fortune* 500.

With respect to industry sector, there are four sectors in which a privacy policy is posted by all firms. These include healthcare, commercial banks, chemicals, and pharmaceuticals. The sector with the lowest participation is mining, crude-oil production with 64% of the 14 firms posting a privacy policy. All other sectors have at least 80% of its firms posting a policy. With respect to policy composition, there are variations in implementation. In terms of notice/awareness, healthcare (100% of firms), chemical (100% of firms), and pharmaceutical companies (100% of firms) have the highest sector immersion. Relative to choice/consent, pharmaceutical (100% of firms), commercial bank (95% of firms), and telecommunication (91% of firms) companies have the highest sector immersion. With respect to access/participation, pharmaceutical (92% of firms) and telecommunication companies (91% of firms) have the highest sector immersion. In terms of security/integrity, pharmaceutical (92% of firms) and general merchandiser (90% of firms) companies have the highest sector immersion. When examining which sector has the highest overall use of the four principles, pharmaceutical firms lead the way. Specifically, 100% of pharmaceutical firms provide notice/awareness, 100% describe choice/consent, 92% discuss access/participation, and 92% address security/integrity.

Table 4. Policy Usage and Composition by Industry Sector

Industry Sector	Number of Firms in Fortune 500	Percent With Policy	Percent With Notice	Percent With Choice	Percent With Access	Percent With Security
Insurance	38	89%	87%	76%	55%	76%
Food Industry	32	91%	91%	84%	75%	66%
Specialty Retailer	28	93%	93%	82%	79%	75%
Wholesaler	27	96%	93%	78%	48%	78%
Utilities: Gas and Electric	23	87%	91%	70%	57%	61%
Healthcare	20	100%	100%	75%	70%	85%
Commercial Bank	19	100%	95%	95%	79%	84%
Chemicals	15	100%	100%	80%	67%	73%
Motor Vehicles & Parts	15	80%	73%	53%	27%	20%
Mining, Crude-Oil Production	14	64%	64%	43%	43%	36%
Pharmaceuticals	13	100%	100%	100%	92%	92%
Aerospace & Defense	11	82%	91%	73%	73%	73%
Computers	11	91%	91%	82%	82%	73%
Petroleum Refining	11	82%	82%	73%	55%	36%
Telecommunications	11	91%	91%	91%	91%	82%
General Merchandiser	10	90%	90%	70%	80%	90%
Total (60% of Firms)	298					

Finally, Spearman Rho correlations were calculated to determine if there are potential relationships between each policy principle and industry sector (Table 5). The Spearman Rho correlation was utilized because it is a nonparametric measure of statistical dependencies between two variables [1]. Results found that one principle had a significant correlation with industry sector. Notice/awareness had a significant correlation at the .05 level.

Table 5. Spearman Rho Correlations Between Policy Principle and Industry Sector

Principle	Correlation With Industry Sector
Notice/Awareness	-.103*
Choice/Consent	-.070
Access/Participation	-.079
Security/Integrity	-.081

* Correlation is significant at .05 level (2-tailed).

CONCLUSIONS, IMPLICATIONS, AND LIMITATIONS

Results indicate that most of the *Fortune* 500 firms have a privacy policy posted online. Specifically, 90% of the firms have a policy link on their home page while 4% of firms have the policy located on a web page not linked to the home page. This is a striking increase from 2002 in which 52% of the *Fortune* 500 firms posted a policy and from 2006 in which 79% posted a policy.

The posting of a policy, however, varies by firm size. For example, while all of the *Fortune* 1-100 firms have a posted privacy policy, only 91% of the *Fortune* 301-500 firms have a posted policy. In terms of policy composition, the principles of notice/awareness and choice/consent, respectively, are the most common principles addressed in the privacy policy for all firm size categories. The principles of access/participation and security/integrity are far less common for each size category. Overall, the *Fortune* 201-300 firms include the highest percentage of policies addressing notice/awareness (96% of firms), access/participation (70% of firms), and security/integrity (80% of firms) while the *Fortune* 1-100 firms include the highest percentage of policies addressing choice/consent (92% of firms).

A further examination of policies finds the inclusion of additional practices and policies. These include the practices of cookies/beacons for tracking and SSL/TLS security and policies covering mobile applications and children. Relative to firm size categories, cookies or beacons are described in 72% of firm policies (*Fortune* 301-400) to 92% of firm policies (*Fortune* 1-100). SSL/TLS security measures are, on the other hand, described in only 17% of firm policies (*Fortune* 401-500) to 25% of firm policies (*Fortune* 201-300). Mobile application policies vary from 19% of firm policies (*Fortune* 301-400) to 44% of firm policies (*Fortune* 1-100). Finally, children policies are included in 48% of firm policies (*Fortune* 301-400) to 71% of firm policies (*Fortune* 1-100).

Results also show that the use of the posting of privacy policies and inclusion of policy components varies by industry sector. For example, 87% of gas and electric utility companies post a policy and 91% of firms provide notice/awareness, 70% describe choice/consent, 57% discuss access/participation, and 61% address security/integrity. This is different from the insurance industry in which 89% of firms post a policy, 87% of firms provide notice/awareness, 76% describe choice/consent, 55% discuss access/participation, and 76% address security/integrity. Overall, there are no two industries with identical usage patterns. The highest percentage implementation sector, however, is the pharmaceutical sector. When examining policy posting, the highest percentage implementers are healthcare, commercial banking, chemical, and pharmaceutical firms, each with 100% of firms. When examining the highest percentage of firms within an industry sector implementing the four principles, results vary by sector. With respect to notice/awareness, the highest sectors are health care, chemical, and pharmaceutical firms. With respect to choice/consent, the highest sectors are commercial bank and pharmaceutical firms. With respect to access/participation, the highest sectors are pharmaceutical and telecommunication firms. With respect to security/integrity, the highest sectors are pharmaceutical and general merchandiser firms. Finally, Spearman Rho correlations with industry sector found that notice/awareness had a correlation significant at the .05 level.

Implications

There are three important implications as a result of these findings:

1. One implication is that while there has been a dramatic increase in the number of *Fortune* 500 firms posting a privacy policy to their website and that the inclusion percentages of the four FIP principles have shifted, it is possible that firms may be designing policies reactively based upon the current stakeholder concerns. For example, from 2002 to 2014, the percentage of firms posting a policy increased by 81% to 94% of firms. Moreover, the primary principles shifted from awareness/notice (98% of firms) and security/integrity (71% of firms) in 2006 to awareness/notice (86-96% of firms) and choice/consent (72-92% of firms) in 2014. In the period after the September 11, 2001 terrorist attacks, it could be surmised that stakeholders were highly concerned about security. In the last decade, however, there has been the trend of user empowerment and choice during the social media explosion. It remains to be seen if the recent data thefts will again result in the increasing focus of security/integrity in policies in an attempt to reassure stakeholders. A more effective approach, however, would be to employ a proactive strategy in which all four FIP principles are thoroughly addressed in the firm's privacy policy. This would allow firms to more easily adapt to future stakeholder demands.

2. A second implication is with regard to organization size. The *Fortune* 1-100 had the highest percentage of firms posting a privacy policy online. On the other hand, the *Fortune* 301-500 had the lowest percentage of firms. In addition, there are variations in policy composition when examining size. Notice/awareness, for example, ranged from 86% of the *Fortune* 401-500 firms to 96% of the *Fortune* 201-300 firms and security/integrity ranged from 64% of the *Fortune* 1-100 firms to 80% of the *Fortune* 201-300 firms. Further evidence is also found when examining the use of additional practices and policies. For instance, 92% of the *Fortune* 1-100 firms describe cookies or beacons while only 72% of the *Fortune* 301-400 firms do the same. For the most part, as organization size decreases, the description of cookies/beacons, the implementation of SSL/TLS security, the inclusion of mobile application policies, and the detailing of children policies also decreases. It is possible that the largest organizations perceive a greater risk from possible litigation and/or have a larger and more varied stakeholder base that needs to be addressed. Overall, these results imply that smaller firms are at greater risk and that it is important these firms implement a privacy policy and evaluate its composition.

3. A third implication is with respect to industry sector. Notice/awareness had a significant statistical correlation with industry sector. In addition, the inclusion of the four FIP principles varied by industry sector. Notice/awareness, for example ranged from 82% of petroleum refining firms to 100% of health care firms and access/participation ranged from 55% to 70% of the same firms. Moreover, when examining any sector, there are wide differences. While 55% of insurance firms include access/participation, 76% address choice/consent and security/integrity, and 87% describe notice/awareness. Results suggest that each industry sector may perceive different threats because of its unique existing and potential stakeholders. Of importance, results also imply that there may be disadvantages for firms within a given industry sector that may choose not to implement a policy or include all four FIP principles.

The limitations of this study are primarily a function of the research methodology and analyses. First, the study was limited to the *Fortune* 500 firms. As a result, policy posting and composition may be different with regard to medium and small businesses. Second, in an effort to simplify the analysis, only the largest industry sectors (those with at least 10 companies) were examined. Consequently, 40% of the firms were not included in the industry sector analysis. Finally, industry size was segmented into five size categories. Although the categories were made to provide further understanding of policy practices, other size categorizations could be devised to gain additional insight. Overall, however, the study provides rich insight into *Fortune* 500 firms and their privacy policy practices.

REFERENCES

1. Conover, W. J. (1999). *Practical nonparametric statistics*. Hoboken, NJ: Wiley.
2. Fitzgerald, J., Dennis, A., & Durcikova, A. (2012). Business data communications and networking. 11th Edition, John Wiley & Sons, Inc.: Hoboken, NJ.

3. Fortune (2014). Fortune 500 2014. *Money.cnn.com*. Available: http://fortune.com/fortune500/
4. Ickert, D. & McCracken, T. (2013). 2013 Small business technology survey. *nsbl.biz*, 1-14. Available: http://www.nsba.biz/wp-content/uploads/2013/09/Technology-Survey-2013.pdf
5. Junius, D. (2014). Poll: Credit and debit card security breaches not changing people's habits. *Associated Press*, January 26. Available: http://www.ap-gfkpoll.com
6. Kroll (2013). 2013/2014 Global fraud report. *Idgconnect.com*, October 18, 1-48. Available: http://www.idgconnect.com/download/17278/2013-14-global-fraud-report
7. Laudon, K. C. & Traver, C. G. (2015). E-Commerce. 11th Edition, Prentice Hall: Upper Saddle River, NJ.
8. Liu, C. & Arnett, K. P. (2002). An examination of privacy policies in Fortune 500 web sites. *American Journal of Business, 17*(1), 13-22.
9. NCSL (2014). 2014 Security breach legislation. National Conference of State Legislatures, December 23. Available: http://www.ncsl.org/research/telecommunications-and-information-technology/2014-security-breach-legislation.aspx
10. PwC (2013). Key findings from the 2013 U.S. State of Cybercrime Survey. *pwc.com*, June, 1-18. Available: http://www.pwc.com/us/en/increasing-it-effectiveness/publications/us-state-of-cybercrime.jhtml
11. Schwaig, K. S., Kane, G. C., & Storey, V. C. (2006). Compliance to the Fair Information Practices: How are the Fortune 500 handling online privacy disclosures? *Information & Management*, *43*, 805-820.
12. Symantec (2012). New Survey Shows U.S. small business owners not concerned about cybersecurity; Majority Have No Policies or Contingency Plans. *Symantec.com*, October 15. Available: http://www.symantec.com/about/news/release/article.jsp?prid=20121015_01
13. Warren, S. D. & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193-220.
14. Weise, E. & Guynn, J. (2014). 24% of Americans stopped buying online because of breaches. *USA TODAY*, June 3. Available: http://www.usatoday.com/story/tech/2014/06/03/internet-security-survey/9907947/
15. Whittaker, Z. (2014). 2014 In security: The biggest hacks, leaks, and data breaches. *Zdnet.com*, December 28. Available: http://www.zdnet.com/pictures/2014-in-security-the-biggest-hacks-leaks-and-data-breaches