AN EXAMINATION OF PRIVACY POLICIES OF GLOBAL ON-LINE E-PHARMACIES

Dr. Joanne Kuzma
University of Worcester
U.K.

Kate Dobson
University of Worcester
U.K.

Andrew Robinson
University of Worcester
U.K.

ABSTRACT

This paper investigates the differences in privacy policy functions among 90 online pharmacy websites in nine countries in Europe, Asia and North America. Results from this study show that the majority of websites do have privacy policies, but the level of functional protection of consumers varies widely. Even in those countries where strong privacy laws exist, the level of privacy protection adherence is often very low. Most studies of privacy policy issues have concentrated on websites from developed nations, with few studies of the pharmacy industry. A better understanding of this industry, as well as understanding the differences in privacy policy implementation among developing and developed countries, provides important lessons for both businesses and consumers.

Keywords: E-pharmacy, online pharmacies, privacy, healthcare sector, privacy policies.

INTRODUCTION

The number of Web-based online pharmacies has increased dramatically in recent decades due to various pricing and other factors. Online shopping facilitates greater convenience of purchasing and delivery of products. Su et al. (2011) indicate that the growth is also due to the lack of availability of these products in traditional pharmacies in rural areas. However, this growth must be tempered by a variety of issues such as recognition of 'legitimate' sites, lack of legal oversight, and consumer protection and privacy concerns.

When using websites to purchase medicines and pharmaceuticals, consumers are faced with questions about what sort of privacy protection the online firms use to secure their personal information. In an effort to alleviate risks to themselves, consumers must rely on businesses to secure their personal information and notify them of the processes and procedures they take to implement data safety, mostly by means of a privacy policy notification. This research provides new evidence that firms do not always have privacy policies on their websites. If firms do have online policy notifications they often exhibit a dearth of information about the actual data collected and ambiguity in the methods that firms use to collect personal data.

LITERATURE REVIEW

Growth of Online Pharmacies

The number of online pharmacies has grown substantially in the past several years. According to LegitScript (2015), an online pharmacy verification service, there are over 35,000 online pharmacies throughout the world, and between 0.6 and 5.7 percent could be considered legitimate based upon national certification. Internationally, countries have a myriad of legislation based around certification of pharmacies as well as consumer laws to protect consumers using the online firms.

According to James Dudley Management (2012), since 2012, France, Italy and Austria have legitimized the ability for businesses to enter the online pharmacy sector, resulting in a huge

growth in this market. There are currently around 7,000 European authorized e-commerce pharmacy sites, ranging from small independent firms to large global cross-border entities. These cover 482 million Internet users. Countries such as the UK have experienced tremendous growth over the past several years, with the number of UK online pharmacies growing from 56 in 2008, to 211 in 2014 (Statista, 2015).

This growth has also led to changes in the business model for this sector. For example, Austrian and German apothecary chains are partnering with online pharmacies in order to capture a share of this healthcare sector which, until now, has been the exclusive province of pharmacies. According to Brown (2015), the big attraction for high-street pharmacies to add Internet sites to their operational strategy is that the websites can help prop up revenues and provide additional outlet for sales.

Privacy and Trust

Consumer privacy and trust of online firms is a major issue among online consumers (Reay et al., 2009). A survey by the European Commission (2014) found that 70 percent of Europeans were concerned about privacy issues such as the potential use that companies make of the information collected and 90 percent of Europeans say they are concerned with data privacy regarding mobile apps. Johnson (2008) examined Internet use among Canadians and found that almost 80 percent had concerns about privacy. Privacy and trust is a two-way street for both firms and consumers. To gain consumer trust, firms need to implement a variety of methods to convince their customers that personal information obtained through e-commerce transactions will be safe; one method is by using detailed privacy policies (Peterson et al., 2007).

Organizations need to create policies and procedures within the framework of legal requirements. Also, organizations have an ethical obligation to protect their customer's private data. Young (2011) states that firms should develop privacy practices to collect, store and use data judiciously. Additionally, firms should ensure that they follow their stated online privacy policies. McRobb and Rogerson (2004) indicate that a policy's location on the website, its prominence and contents, carry explicit and implicit messages to the consumers about the organization.

Privacy Mechanisms

Peterson et al. (2007) states that there are a variety of privacy mechanisms to increase trustworthiness including privacy policy statements, third-party seal programs, quality of website design and customer testimonials. This research paper concentrates on several specific areas of privacy functions that online firms can use, including standardization, requirement for notice and TRUSTe seals.

According to Kelley et al. (2010), privacy policy formats have a significant impact on consumer's ability to quickly and accurately find information about the site's privacy protection. The authors study found that standardized policies have a positive impact on user's perception, and can benefit users. Current privacy policies often contain long and complicated texts not easily understood by many consumers (Angulo, 2012). Therefore, simplified and standardized privacy policies that consumers understand are beneficial to maintaining a level of trust of personal data safety. A research project by Angulo et al. (2012) presented an approach for designing simplified privacy policies. Results showed that users

understood and appreciated this approach and perceived the benefits for protecting their privacy online.

Legal requirements for privacy and security notifications vary across countries. Most countries do not explicitly require an online privacy statement, but do highly recommend some method of communicating the information to consumers. For example, the UK's Data Protection Act does not specifically mandate use of an online privacy policy, but does require a 'fair processing notice' (Information Commissioner's Office, 2015). An obvious method of providing notice would be a privacy statement on the website.

Legal Standards

According to Reay et al. (2009a), numerous studies have shown that concern for personal privacy is a major impediment to the growth of e-commerce, resulting in consumer watchdog groups calling for more legislation and privacy protection. Many nations have enacted national or regional legislation to safeguard personal privacy for online data protection, although studies have indicated that the legislation is not always adhered to. In North America, the USA, Canada and Mexico all have federal laws dealing with privacy protection to some extent, with additional regional acts in some jurisdictions. Canada has strong privacy laws with 28 federal, provincial and territory privacy statutes that govern personal privacy in the private and public sectors (DLA Piper, 2015a). In June 2015, the Canadian federal government enacted the Digital Privacy Act, which sets clear rules for how personal information can be collected, used and disclosed online (Government of Canada, 2015).

According to IT Law Group (2015), Mexico's Federal Law on the Protection of Personal Data Possessed by Private Persons became effective on July 6, 2010. Online providers are required to have privacy notices that identify if the entity collects data, what data is collected, the purpose for collection and the transfer and retention of data. The United States does not have an overriding national law regulating online privacy. Instead, there are a myriad of state laws and federal guidelines that address online concerns for various groups and industries. The Children's Online Privacy Protection Act (COPPA) requires website owners to protect data of children under 13. According to the National Conference of State Legislators (2015), some states have addressed online privacy in their own jurisdiction. For example, California's Online Privacy Protection Act requires a website operator that collects data about California residents to post a conspicuous privacy policy on its website.

Online privacy for the UK, France and Germany falls within comprehensive European Union (EU) legal directives. Currently, the relevant statutes are the Data Protection Directive (ensures that personal data can only be gathered under strict conditions and for legitimate purposes) and the ePrivacy Directive (ensures that all communications over public networks maintain a high level of privacy) (European Commission, 2015a). All member states are covered under these directives. The directives are set for further reform. In early 2016, the EU is set to approve new levels of data protection and privacy, which could make companies in violation of the law face severe financial penalties and fines of up to 2 percent of revenue. With the reform, companies based outside of Europe will have to apply the same rules if they conduct business with EU consumers (European Commission, 2015b).

Some countries in the EU have enacted their own legislation specifically addressing online pharmacies. Since July 2015, UK online pharmacies selling to the general public must be registered with the Medicines and Healthcare products Regulatory Agency (MHRA), and

must be on the list of UK registered online retail sellers (National Law Review, 2015). They must also display the EU common logo, which is designed to help members of the public identify websites that can legally sell medicines.

According to Centre for Internet & Society (2015) online privacy legislation in India is covered under the Information Technology Act (ITA) 2000. The rules define 'sensitive personal information' and require that any corporate body must publish an online privacy policy, provide individuals with the right to access and correct their information and obtain consent before disclosing sensitive personal information. Currently, Pakistan has no law regarding online privacy protection or any requirement for online privacy policies for website operators (DLA Piper, 2015b).

Singapore's Personal Data Protection Act 2012 (PDPA) comprises of various rules governing the collection, use, disclosure and care of personal data. The PDPA has three main areas of focus:

1. Consent – where firms may collect or disclose personal information only with consent of the individual,
2. Purpose – firms may collect or disclose information only if they have informed individuals of the purpose of the collection,
3. Reasonableness – firms may collect or disclose data under circumstances that would be considered appropriate to a reasonable person. (Personal Data Protection Commission Singapore, 2015).

Currently, there are not specific requirements regarding online privacy policies. However, the general data protection information in the act can be construed to cover areas of online privacy (DLA Piper, 2015c).

The World Intellectual Property Organization (2011) explains that their legislation requires that corporations provide a privacy policy for handling of or dealing in personal information including sensitive personal data or information. The rules state that online policies should be clear and accessible, disclose the type of personal data collected, the purpose for collecting, disclosure policy for the personal data, and security practices and procedures. The policy should be published on the website of the firm and be readily available to consumers.

Prior Studies

A 2012 study by the National Association of Boards Pharmacy (2012) found that of 10,000 websites reviewed, 97 percent did not comply with pharmacy laws and practice standards in the U.S. Proctor (et. al., 2008) conducted a study of privacy policies of seven different categories of websites (including online pharmacies). Their study found that a majority of online pharmacies did have privacy policies, although the number of sites in the study was only six American firms. They found four of the six sites did contain privacy seals (such as TRUSTe), but the actual policy content and readability compared to other industries was poor. A 2006 study of Canadian online pharmacies found that the majority did contain privacy policies, although comprehensiveness of policies differed vastly among the sites (Kuzma, 2006)

Although there have been some studies of the online pharmacy industry, most of the studies relate to North American firms, and many, such as Proctor study in 2008 (Proctor, et. al, 2008) and the 2006 Canadian study (Kuzma, 2006) are dated. There is a dearth of studies

dealing with online firms from other geographical areas such as Asia, Europe, Africa or South America. Thus, this study contributes to the body of knowledge related to privacy policies issues among the global pharmaceutical industry. It contributes to a better understanding of how online privacy policies are used in nine different countries, thus providing lessons in safe practices to consumers in other countries and other industries.

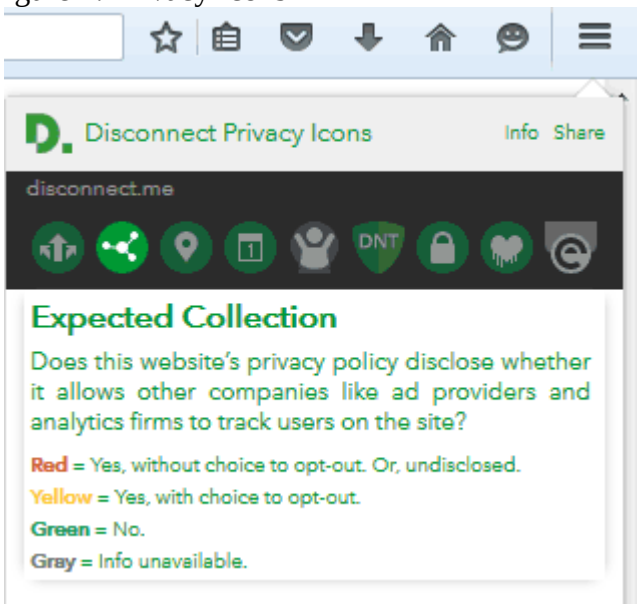
METHODOLOGY

The research in this paper was accomplished by analyzing 90 online pharmacy sites to determine the level of privacy protection for each site. The project consisted of three phases:

1. Choosing privacy factors to analyze
2. Choosing a list of sites
3. Analyzing results

The first phase of this study was to choose a privacy analyzer tool that contained a variety of privacy factors to analyze. The tool had to be either free or low cost due to budget constraints, and needed to contain a viable list of functional factors to review for each website. The firm Disconnect.me (2015) provides a variety of privacy and security protection products, including a free browser extension for Firefox that allows web users to easily understand the privacy policies of websites they are visiting by using a series of privacy icons. Figure 1 illustrates how a series of privacy icons display key elements of privacy policies that would be show at the top right of the Firefox 'Open' menu (Disconnect.me, 2015).

Figure 1: Privacy Icons



Disconnect.me (2015) explains the functions of each of the nine available icons. The first icon is 'expected use', which indicates whether the site's privacy policy discloses whether data it collects about the user is used in ways other than what one would reasonably expect for the site's service. Icons can show on Firefox in various colors, for an easy way for consumers to tell the meaning of the icons:

1. Red = yes, without choice to opt-out, or undisclosed.
2. Yellow = yes, with choice to opt-out.
3. Green = no.

4. Gray = information is unavailable.

The second icon is 'expected collection,' which shows if the policy discloses whether it allows other companies, such as advertising providers and analytics firms, to track users on the site. The color scheme is the same as for the 'expected use' icons. The third icon shows 'precise location,' indicating whether the site tracks a user's geolocation. 'Data retention' is the fourth icon and indicates whether the policy discloses how long they retain personal data (red = no policy, yellow = 12 months, green = 0-12 months, and gray = information unavailable). The fifth icon is 'children privacy' to indicate if the site received TRUSTe's Children Privacy Protection Certification. The sixth icon, 'do not track' shows whether the site complies with a user's Do Not Track browser preference. The next icon is 'SSL support,' showing if the site supports secure communication over HTTPS by default. According to TRUSTe (2015), SSL (Secured Sockets Layer) encryption is a security measure that firms should take while collecting sensitive customer data, thus ensuring customer trust. The eighth icon is 'heartbleed,' which shows if the site is vulnerable to the heartbleed bug, a vulnerability in SSL, (red = vulnerable, yellow=unknown, green = safe, gray = NA). The last icon is 'TRUSTe certified, 'showing if the site has obtained TRUSTe's certification.

In addition to collecting data from the disconnect.me software, the research also reviewed each site for a privacy policy. Care had to be taken to do a thorough search of the links from the main home page, as sometimes privacy policy information could be found on a different named page, such as 'terms and conditions' or 'legal.'

The second phase of this study was to select 90 online pharmacies in three different geographical locations (Asia, North America and Europe). For each of these areas, three countries were selected, and 10 different online pharmacies for each country were chosen.

The methodology used to select the countries and pharmacies was based on a Google search. The search phrase consisted of three words, the first two words being 'online pharmacies' and the third word was the name of the country. Thus, a search of pharmacies for India would be 'online pharmacies India.' If a country had at least 30 online pharmacies in the search result, it was considered a viable choice. A second consideration was to actually ensure that the results of the pharmacy links were viable pharmacies that sold products online, as opposed to informational websites. In some cases, countries used different terms for 'pharmacy', so the national preferred wording was used. For example, the common German term was 'apothoke' and the French term was 'farmacia'.

RESULTS

Table 1 displays the results for three countries in Asia: India, Pakistan and Singapore, as well as a column for the total. India had the highest number of sites (90 percent) containing a privacy policy somewhere within their website. Pakistani and Singaporean sites had 50 percent and 40 percent rates of including privacy policies within pharmacy sites respectively, while the average for Asian countries was 60 percent.

Results for 'expected use', 'expected collection', 'precise location', 'data retention' and 'do not track' statistics were all similar with all sites having the result of 'information unavailable' for all attempts to track. The results for 'children privacy' showed that no sites had received TRUSTe's Children's Privacy Protection Certification. There are 50 percent of Indian pharmacies considered 'safe' from the heartbleed bug, while the vast majority of

Pakistani and Singaporean sites (90 percent) are vulnerable to the bug. Most Indian sites (60 percent) have HTTPS secure communications by default, while 10 percent of Pakistani sites and 40 percent of Singaporean sites were considered secure. None of the sites received TRUSTe's Privacy Certification.

Table 1: Asian Privacy Results

	India	Pakistan	Singapore	Total
Policy exists	9 (90%)	5 (50%)	4 (40%)	18 (60%)
Expected use	Un- 10 (100%)	Un -10 (100%)	Un - 10 (100%)	Un - 30 (100%)
Expected collection	Un- 10 (100%)	Un -10 (100%)	Un - 10 (100%)	Un - 30 (100%)
Precise location	Un- 10 (100%)	Un -10 (100%)	Un - 10 (100%)	Un - 30 (100%)
Data retention	Un- 10 (100%)	Un -10 (100%)	Un - 10 (100%)	Un - 30 (100%)
Children privacy	No- 10 (100%)	No -10 (100%)	No - 10 (100%)	No - 30 (100%)
Do not track	Un- 10 (100%)	Un -10 (100%)	Un - 10 (100%)	Un - 30 (100%)
SSL support	6 (60%)	1 (10%)	4 (40%)	11 (36%)
Heartbleed - safe	5 (50%)	1 (10%)	1 (10%)	7 (23%)
TRUSTe	0	0	0	0 (0%)

Table 2 shows the results for three countries in North America: Canada, Mexico and the USA. All Canadian and American pharmacy sites had privacy policies, while only 60 percent of Mexican sites had them. Canadian and Mexican sites did not have available information for the expected use, collection, location, data retention and children privacy functions. However, results for American sites for these functions were higher, with two pharmacy sites having positive scores for expected use and expected collection, with choice to opt-out. For 'precise location', one site did have this function, but without choice to opt-out. Two American sites disclosed their data retention policy, and kept data more than 12 months.

Table 2: North America Privacy Results

	Canada	Mexico	USA	Total
Policy exists	10 (100%)	6 (60%)	10 (100%)	26 (87%)
Expected use	Un- 10 (100%)	Un -10 (100%)	Un - 8 (80%) YW – 2 (20%	Un - 28 (93%) YW – 2 (7%)
Expected collection	Un- 10 (100%)	Un -10 (100%)	Un - 8 (80%) YW – 2 (20%	Un - 28 (93%) YW – 2 (7%)
Precise location	Un- 10 (100%)	Un -10 (100%)	Un - 9 (90%) WO – 1 (10%)	Un - 29 (97%) WO – 1 (3%)
Data retention	Un- 10 (100%)	Un -10 (100%)	Un - 8 (80%) 12+ – 2 (20%)	Un - 28 (93%) 12+ – 2 (7%)
Children privacy	No- 10 (100%)	No -10 (100%)	No - 10 (100%)	No - 30 (100%)
Do not track	Un- 10 (100%)	Un -10 (100%)	Un - 10 (100%)	Un - 30 (100%)
SSL support	9 (90%)	5 (50%)	9 (90%)	23 (77%)
Heartbleed - safe	3 (30%)	4 (40%)	5 (50%)	12 (40%)
TRUSTe	1 (10%)	0 (0%)	1 (10%)	2 (7%)

Table 3 displays privacy results for three European countries: the UK, France and Germany. The majority of sites in each county do have a privacy policy, with the UK possessing the most at 80 percent, Germany at 60 percent and half the sites in France. Results for expected use, collection, location, data retention, children privacy and tracking are all unavailable for all sites in all countries. SSL support is good in the UK with 90 percent compliance, while Germany has 50 percent and France only 20 percent. Results are similar for the heartbleed bug where it is most safe for UK sites (80 percent), with fewer sites in Germany (30 percent) and France (10 percent). None of the European sites have TRUSTe certification.

Table 3: Europe Privacy Results

	UK	France	Germany	Total
Policy exists	8 (80%)	5 (50%)	6 (60%)	19 (63%)
Expected use	Un- 10 (100%)	Un -10 (100%)	Un - 10 (100%)	Un - 30 (100%)
Expected collection	Un- 10 (100%)	Un -10 (100%)	Un - 10 (100%)	Un - 30 (100%)
Precise location	Un- 10 (100%)	Un -10 (100%)	Un - 10 (100%)	Un - 30 (100%)
Data retention	Un- 10 (100%)	Un -10 (100%)	Un - 10 (100%)	Un - 30 (100%)
Children privacy	No- 10 (100%)	No -10 (100%)	No - 10 (100%)	No - 30 (100%)
Do not track	Un- 10 (100%)	Un -10 (100%)	Un - 10 (100%)	Un - 30 (100%)
SSL support	9 (90%)	2 (20%)	5 (50%)	16 (53%)
Heartbleed - safe	8 (80%)	1 (10%)	3 (30%)	12 (40%)
TRUSTe	0	0	0	0 (0%)

Overall results show a wide difference in geographic regions and even countries within each region. Most of the countries (except Singapore) have at least 50 percent of their site displaying privacy policies with North American countries the highest at 93 percent while European and Asian results are similar at 63 and 60 percent. A wide difference in statistics exists, with some countries like Singapore only showing 40 percent of sites containing privacy policies while Canadian and American sites have 100 percent compliance. A surprising result is that France (50 percent) and Germany (40 percent) have such low numbers, especially in light of the European Union's strong privacy laws.

Results for functions of expected use, expected collection, precise location, data retention, children privacy and tracking were consistently low or non-existent for the vast majority of sites, with only a minimal number in the USA displaying this information. SSL support had a wide range of statistics throughout the globe. North American sites showed the greatest number of sites with SSL support with an overall average of 77 percent. European countries were next at 53 percent with Asia showing results of only 36 percent.

For the heartbleed bug function, there was a very wide range of protection. UK sites had a high of 80 percent considered 'safe', followed by the USA and India with 50 percent of sites were safe. However, Pakistan, Singapore and France all had a low score of only 10 percent of the sites were safe. TRUSTe privacy certification was one of the worst-performing categories, with only two sites (one in Canada and one in the USA) displaying certification.

DISCUSSION AND CONCLUSIONS

The aim of this research was to discern the differences in privacy policies among online pharmacies in nine different countries to determine if there was any commonality among implementation. The search showed a wide divergence in countries regarding the utilization of policies. Most of the firms in each geographical region did provide policies on the sites (average of 70 percent overall), but policy coverage was quite diverse and generally of poor quality. Few sites informed consumers about their expected use of data, expected collection, location, data retention, children's privacy or tracking. Only two sites in North America contained TRUSTe seal of privacy approval. Sites were marginally better in showing that they have SSL support for e-commerce transactions with 55 percent of sites displaying this on their policy notification page.

What was most striking is that even in those countries that had strong privacy protection laws, online pharmacies based in those countries did not necessarily adhere to legislation, thus leaving consumers at risk and confused about privacy protection, and site owners at risk of legal action. Legal mandates are especially strong in European and North American countries compared to Asian countries studied. Yet, even with strong legislation, only 63 percent of European sites possessed policies, only marginally better than 60 percent of Asian sites. This research shows that legal mandates are not being followed by the online pharmacy industry. The findings show that online pharmacy owners across the globe have a significant amount of work to do in order to address their consumer's online privacy needs with regards to providing detailed information on their privacy statements. A further phase of this study could be added to examine the reasons why sites in this industry are not following legal due process, and perhaps determining why some privacy functions are shown on the majority of sites, while others are not.

REFERENCES

Angulo, J. (2012) 'Usable privacy for digital transactions: Exploring the usability aspects of three privacy enhancing mechanisms', University dissertation, Karlstads university.

Angulo, J., Fischer-Hübner, S., Wästlund, E. and Pulls, T. (2012). Towards usable privacy policy display and management. *Information Management & Computer Security*, 20(1), p. 4 – 17.

Brown, E. (2015) *Online Pharmacies Crash the Party*, [Accessed 8th March 2016] Available from: http://www.politico.eu/article/online-pharmacies-crash-the-party/.

Capistrano, E, and Chen, J. (2015) 'Information privacy policies: The effects of policy characteristics and online experience', *Computer Standards & Interfaces*, 42, p. 24-31.

Centre for Internet & Society (2015) *Internet Privacy in India*, [Accessed 10th March 2016] Available from: http://cis-india.org/telecom/knowledge-repository-on-internet-access/internet-privacy-in-india.

Desai, M., Desai, K., and Phelps, L. (2012) 'E-commerce policies and customer privacy: a longitudinal study (2000-2010)', *Information Management & Computer Security*, 20(3), p.222 – 244.

Disconnect.me (2015) *Disconnect Privacy Icons*, [Accessed 27th March 2016] Available from: https://disconnect.me/icons.

Information Commissioner's Office (2015) *Processing personal data fairly and lawfully (Principle 1)*, [Accessed 8th May 2016] Available from:m https://ico.org.uk/for-organisations/guide-to-data-protection/principle-1-fair-and-lawful/.

Kelley, P.G., Cesca, L., Bresee, J. and Cranor, L.F. (2010) 'Standardizing privacy notices: an online study of the nutrition label approach', *Proceedings of the 28th International Conference on Human Factors in Computing Systems*, ACM, New York, NY, p. 1573, https://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab09014.pdf.

DLA Piper (2015a), *Law in Canada*, [Accessed 8th March 2016] Available from: http://www.dlapiperdataprotection.com/#handbook/law-section/c1_CA.

DLA Piper (2015b), *Law in Pakistan*, [Accessed 8th March 2016] Available from: http://dlapiperdataprotection.com/#handbook/law-section/c1_PK.

DLA Piper (2015c) *Law in Singapore*, [Accessed 8th March 2016] Available from: http://dlapiperdataprotection.com/#handbook/online-privacy-section/c1_SG.

European Commission (2014) *Progress on EU data protection reform now irreversible following European Parliament vote*, [Accessed 9th May 2016] Available from: http://europa.eu/rapid/press-release_MEMO-14-186_en.htm.

European Commission (2015a) *Online Privacy*, [Accessed 9th June 2016] Available from: https://ec.europa.eu/digital-agenda/en/online-privacy.

European Commission (2015b) *Stronger data protection rules for Europe*, [Accessed 1st May 2016] Available from: http://europa.eu/rapid/press-release_MEMO-15-5170_en.htm.

Government of Canada (2015) *New Law to Protect the Personal Information of Canadians Online*, [Accessed 1st June 2016] Available from: http://news.gc.ca/web/article-en.do?nid=988939.

IT Law Group (2015) *Mexico's New Federal Law on the Protection of Personal Data*, [Accessed 1st June 2016] Available from: http://www.itlawgroup.com/resources/articles/98-mexicos-new-federal-law-on-the-protection-of-personal-data.

James Dudley Management (2014) *The Future for Pharmacy Exploring Strategies for Competitive Success*, [Accessed 9th June 2016] Available from: http://www.james-dudley.co.uk/downloads/presentations/Future-of-pharmacy-Factors-for-Success-2015.pdf.

Johnson, E. (2008) *Privacy and Security Concerns Related to Internet Use in Canada*, PhD Thesis, Keele University.

Kuzma, J. (2006) *Privacy Policies: A Study of Their Use Among Canadian Online Pharmacies*, PhD Thesis, Nova Southeastern University.

Legitscript (2015) *Legistscript Home Page*, [Accessed 9th June 2016] Available from: https://www.legitscript.com/.

McRobb, S., and Rogerson, S. (2004) 'Are they really listening?', *Information Technology & People*, 17(4), p. 442 – 46.

National Association of Boards Pharmacy (2012) Retrieved from *NABP: Buying Medicine Online*, [Accessed 9th June 2016] Available from: http://www.safemedsonline.org/resource/nabp-buying-medicine-online/.

National Conference of State Legislators (2015) *State laws related to Internet privacy*, [Accessed 9th June 2016] Available from: http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.

National Law Review (2015) *Mandatory Registration and Logo for UK Sales of Medicines*, [Accessed 12th June 2016] Available from:

http://www.natlawreview.com/article/mandatory-registration-and-logo-uk-online-sales-medicines.

Peterson, D., Meinert, D., Criswell, J. and Crossland, M. (2007), 'Consumer trust: privacy policies and third-party seals', *Journal of Small Business and Enterprise Development*, Vol. 14, No. 4 p. 654 – 669.

Proctor, R, Ali, M, and Vu, K. (2008) 'Examining Usability of Web Privacy Policies', *International Journal Of Human-Computer Interaction*, 24(3), p. 307-328.

Personal Data Protection Commission Singapore (2015) *Legislation and Guidelines – Overview*, [Accessed 15th May 2016] Available from: https://www.pdpc.gov.sg/legislation-and-guidelines/overview.

Reay, I., Dick, S., and Miller, J. (2009) 'A large-scale empirical study of P3P privacy policies: Stated actions vs. legal obligations', *ACM Transactions on the Web*, 3(2), p. 6:1 – 6:33.

Statista (2015) *Number of Distance Selling/Mail Order pharmacies in England from 2008 to 2014*, [Accessed 9th June 2016] Available from: http://www.statista.com/statistics/418249/distance-selling-pharmacies-in-england/.

Su, L., Huang, W., and Leung, J. (2011) 'Development and management of online pharmacies in China', *Journal of Medical Marketing*. 11(3), p. 197-203.

TRUSTe (2015) Proctecting Customer Information Online [Accessed 7th June 2016] Available from: https://www.truste.com/resources/privacy-best-practices/

World Intellectual Property Organization (2011) *India – Ministry of Communications and Information Technology*, [Accessed 23rd April 2016] Available from: http://www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf.

Young, J. (2011) 'Commitment analysis to operationalize software requirements from privacy policies', *Requirements Engineering*, 16(1), p. 33-46.