Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 37 (2014) 348 – 355

Procedia Computer Science

The 4th International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare (ICTH-2014)

A privacy policy comparison of health and fitness related mobile applications

Mark Rowan[1] and Josh Dehlinger

Department of Computer and Information Sciences, Towson University, Towson, MD, 21252 USA

Abstract

Many mobile device end users believe that privacy is important when dealing with personal health-related information, but the challenge is to develop privacy policies in a meaningful way so that mobile software application developers can adequately meet the requirements of their intended end users. Comprehensive privacy policies, which meet self-regulatory guidelines of increasing transparency on data collection, are often written in a way that average mobile users cannot understand or completely ignore. This paper provides the results of a privacy policy comparison including application permissions requested and several readability metrics used to assess the current state of privacy policies in the health and fitness mobile application market. Our analysis indicates that developers may not be considering their end-users' reading comprehension levels and specific application permissions are not adequately addressed when developers are creating their privacy policies.

Peer-review under responsibility of the Program Chairs of EUSPN-2014 and ICTH 2014.

Keywords: Privacy Policy; Readability; Mobile Applications; Health and Fitness; Trust and Privacy

1. Introduction

Recent headlines like, "This Flashlight Android app has been secretly and illegally sharing your personal data with advertisers" [1], "Android's app permissions were just simplified-now they're much less secure" [2] and "Users beware: leaks from health websites, apps cause for concern" [3] may influence end users to mistrust mobile applications and discourage their use. Microelectromechanical sensors (i.e., accelerometer, pressure, light sensors, etc.) in mobile phones can inform applications about its environment and be used by mobile applications in a variety of ways. For example, end users can install health and fitness applications on their mobile phones or use companion

[1] Corresponding author. Tel.: 011-1-410-704-2633; fax: 011-1-410-704-3868.
E-mail address: mrowan2@students.towson.edu

Peer-review under responsibility of the Program Chairs of EUSPN-2014 and ICTH 2014.
doi:10.1016/j.procs.2014.08.051

wearable computing devices to track their own well-being (e.g., diet, fitness goals, pregnancy trackers, etc.) and then intentionally share their results with friends, family, coaches, and physicians. Personal health and fitness has become social for many end users for motivational purposes, reporting progress and goal attainment.

It has been reported that health and fitness applications are playing a pivotal role in changing the utility of mobile devices (i.e., tablets, phones) into medical instruments that capture blood test results, glucose readings, medical images and other medical information to better enable physicians and patients to manage and monitor health information [4]. The recent trend in wearable medical devices with biosensors is causing concern in the healthcare community about misdiagnoses that could have serious concerns for consumers [5, 6]. This uneasiness is amplified by the fact that there is no requirement for application developers to have any healthcare experience or fitness certification when creating and publishing health and fitness mobile applications. Many mobile application developers do not have the resources for legal counsel and may be more likely to make false claims to patients without seeking Food and Drug Administration (FDA) clearance [6] or lack the knowledge about privacy when handling personal health information of end users in some situations [7].

A major challenge is to improve transparency for end users about commercial data practices of mobile applications that collect, store and transfer personal information by presenting information in effective privacy policies. Readability is concerned with the ease with which a person can read (i.e., to extract, evaluate, and use information from a text source [8]. The inability to read and understand health information, privacy policies or terms of service agreements can have serious consequences for people by sharing personal information with the software application developer, publisher and some third parties. Privacy concerns have been raised that third party use of personal health information could lead to possible employment discrimination, loss of insurance coverage, higher insurance premiums, or other privacy intrusions [9]. The U.S. Federal Trade Commission (FTC) recommends that all users read privacy policies to understand how an application or website maintains accuracy, access, security, and control of personal information it collects and whether it provides information to third parties [10]. The FTC recently announced that a simple investigation into 12 popular health and fitness applications found them sending users' personal information (i.e., precise health metrics about the end users) to 76 different third parties [11].

The U.S. Food and Drug Administration (FDA) has stated that they will regulate mobile applications that do the same thing as traditional medical devices, which is intended for use in the diagnosis, cure, mitigation, treatment or prevention of disease or intended to affect the structure or function of the body of man or other animals [12]. The Privacy Rule of Health Insurance Portability and Accountability Act (HIPAA) defines protected health information (PHI) as individually identifiable health information held or transmitted by a covered entity (e.g., health care providers, health plans, health care clearinghouse) or its business associate, in any form or media [13]. Generally, software applications specifically for the end user would not be subject to HIPAA. If an end user shares the information with a HIPAA covered entity (e.g., CVS Pharmacy), then the information would become subject to HIPAA compliance [7].

There have been previous studies exploring privacy issues with mobile technologies related to healthcare, including [14, 15] and work on assessing privacy risks with consumer mobile health and fitness applications, such as [16]. Privacy policies are not an effective tool for notifying end users about data collection, storage and transmission practices of mobile applications. There are challenges with the perceived cost in time and effort in reading privacy policies [17], problems with valuation of end-user personal data [18], as well end-user reading comprehension challenges with privacy policies and terms of service [19, 20]. Also of note, a 2007 study found 75% of consumers think that as long as a website has a privacy policy means that the website will not share data with third parties [21].

This paper provides the results of a privacy policy comparison including Android application permissions requested and several readability metrics used to assess the current state of privacy policies in the health and fitness mobile application market. The analysis indicates that developers may not be considering their end-users reading comprehension levels when creating their privacy policies. An inability to understand privacy policies could lead to negative consequences, including end-users inappropriately sharing personal health information or simply an inability by end-users to understand the privacy policy may lead to end-users not installing their applications due to privacy concerns. The contribution of this paper is an assessment of privacy policies for 20 popular Android mobile applications dealing with health and fitness, as well as a comparison of their requested permissions. It is relevant for businesses and software developers to improve transparency to end-users and possibly create more effective privacy policies that could alleviate end-users' concerns over the uses of their personal information.

The rest of this paper is organized as follows. Section 2 presents the research methodology used in this work. Section 3 provides a summary of the readability test results and some observations from the privacy policy comparison. Section 4 offers a conclusion and suggests future work.

2. Research Methodology

A non-exhaustive keyword search for *free health fitness* was conducted in early June 2014 of Google Play's market for twenty popular (i.e., over one million installations) health and fitness related applications that collect personal information (i.e., location). A previous survey of 584 university students indicated that the majority of mobile device end-users do not completely read privacy policies, but yet reported that they would be very concerned if their location was shared with a third party [22]. Inclusion criteria for this study encompassed free English language applications requesting the location permission and over one million installations. Exclusion criteria for this study included non-English applications, or did not request location permission, or had less than one million installations. Free applications were the focus of this study because of a curiosity about the developer's revenue model and anecdotal evidence indicating an increased reliance of using third parties (e.g., advertising networks).

2.1 Android Application Permissions

During normal operations, the Android operating system sandboxes applications from each other and applications must explicitly request to share resources, data and device features (i.e., GPS, contacts, camera, etc.). Anecdotal evidence has indicated that some Android mobile device users are sometimes confused about the application permissions model [23]. Consumers have the ability to review an application's required permissions in the Google Play store under the Additional Information listing. The application's permissions will display with an icon and a brief explanation of the resource or device feature used if the end-user installed the perspective application. Google recommends that end-users review permissions before downloading an application [24]. Google Play has recently attempted to simplify permissions by grouping them into related permissions and the Google Play support pages give the following overview of the thirteen Android Permission groups [24]. Some critics have challenged this simplification of grouping permissions by warning that an initial installation of an application with basic permissions could be later modified to a more advanced permission within the same group during a future update without the end-user's realization [2]. Below is the permission group information that Google provides in their Google Play support pages [24]:

1. **In-Application Purchases**: An application can ask you to make purchases inside the application.
2. **Device and Application History**: An application can use one or more of the following: read sensitive log data; retrieve system internal state; read web bookmarks and history; and/or retrieve running applications.
3. **Cellular Data Settings**: An application can use settings that control mobile data connections and potentially the data received.
4. **Identity**: An application can use account and/or profile information on a device.
5. **Contacts/Calendar**: An application can use a device's contacts and/or calendar information.
6. **Location**: An application can use a device's location, including approximate location (network-based) or precise location (GPS and network-based).
7. **SMS**: An application can use a device's short message service and/or multimedia messaging service.
8. **Phone**: An application can use the device's phone and/or its call history.
9. **Photos/Media/Files**: An application can use files or data stored on a device.
10. **Camera/Microphone**: An application can use a device's camera and/or microphone.
11. **Wi-Fi connection information**: An application can access a device's Wi-Fi connection information, like if Wi-Fi is turned on and the name(s) of connected devices.
12. **Device ID and call information**: An application can access a device Identities, phone number, phone status, and the number connected by a call.
13. **Other**: An application can use custom settings provided by a device manufacturer or application-specific permissions.

Finally, the support pages for permissions inform end-users that the Android operating system may introduce new capabilities and features in the future. It was noted that Google Play provided the most common permissions but many other application permissions and capabilities can be found on Android developer websites (i.e., Bluetooth, read/write bookmarks and history, development tools that test access to protected storage, etc.), which fall under the "Other" permission group. Permissions groups will continue to change as new capabilities are added to the Android operating system and mobile device capabilities.

2.2 Readability Tests

Readability tests are used to assess the difficulty of the vocabulary and sentence structures in English written material. Readability tests do not measure how well people understand material. Readability tests have been challenged because they can only measure the surface characteristics of text and do not measure qualitative factors such as: reader interest/enjoyment, sentence composition and structure, vocabulary selection and overall comprehensibility of the examined text. It has been recommended that documents intended for health or safety instructions be written at the 5th grade level and documents for the general public be written at the 9th grade level [25]. Related work assessing the readability of privacy policies and terms of service for popular websites was conducted by [20] and the open source tool, Text-Statistics [26], was selected for privacy policy readability testing. In preparation for the reading tests, section headings, hyperlinks, addresses and dates were removed to improve the results of the reading tests on the actual text body of the privacy policies.

3. Results

The survey results of each application's requested permission groups are presented, and then followed by the descriptive statistics for readability tests. Notable privacy policy attributes are summarized in Section 3.3.

3.1 Android Permissions

Developers are encouraged to minimize the number of permissions that their applications request for the following reasons: reducing risk of inadvertently misusing permissions, improving user adoption and making the application less vulnerable for attackers [27]. A comparison of requested Android permissions by the permission groups (cf. Section 2.1) can be seen in Table 1 in order from most to least requested groups. Note that multiple capabilities exist within a group and future updates may add or remove permissions within the groups.

Table 1. Comparison of Android Permission Groups requested.

Application	1	2	3	4	5	6	7	8	9	10	11	12	13	Total
Endomondo Sports Tracker	X			X	X	X		X	X			X	X	**8**
RunKeeper - GPS Track Run Walk	X			X	X	X		X	X	X			X	**8**
Runtastic Running & Fitness	X	X		X		X			X	X		X	X	**8**
HealthTap				X	X	X	X		X			X	X	**7**
Nike+ Running				X	X	X		X	X			X	X	**7**
Noom Weight Loss Coach	X			X		X			X	X		X	X	**7**
Weight Watchers Mobile		X		X		X			X	X		X	X	**7**
BabyBump Pregnancy Free	X	X				X			X			X	X	**6**
Calorie Counter -MyFitnessPal					X	X				X	X	X	X	**6**
CVS/pharmacy						X			X	X	X	X	X	**6**
Daily Workouts FREE				X		X			X		X	X	X	**6**
Lose It!	X			X		X			X	X			X	**6**
My Tracks				X	X	X			X			X	X	**6**
Workout Trainer	X			X		X			X			X	X	**6**
iTriage Health					X	X			X		X		X	**5**
miCoach train & run		X				X			X			X	X	**5**
Period Tracker (Pink Pad)	X					X			X			X	X	**5**
Sports Tracker	X					X			X			X	X	**5**
Strava Running and Cycling	X			X		X			X				X	**5**
WebMD for Android						X		X	X				X	**4**

3.2 Readability Test Results

This section describes the surface text statistics for the privacy policies and then provides an overview of the readability tests. The results of the text statistics (e.g., Characters per Word (CpW), Syllables per Word (SpW) and Words per Sentence (WpS)) are presented with an estimated page length for the associated policies from longest to shortest (cf. Table 2).

Table 2. Privacy Policy Text Statistics.

Application	Characters	Syllable	Words	Sentences	CpW	SpW	WpS	Pages
Weight Watchers Mobile	28156	9629	5494	219	5.1	1.8	25.1	11.21
CVS/pharmacy	22213	7400	4590	179	4.8	1.6	25.6	9.37
iTriage Health	24819	8317	4587	170	5.4	1.8	27.0	9.36
WebMD for Android	21483	7143	4416	169	4.9	1.6	26.1	9.01
Calorie Counter -MyFitnessPal	14831	4973	2761	110	5.4	1.8	25.1	5.63
Daily Workouts FREE	13006	4420	2489	76	5.2	1.8	32.8	5.08
My Tracks	11784	3905	2285	115	5.2	1.7	19.9	4.66
BabyBump Pregnancy Free	11246	3819	2252	100	5.0	1.7	22.5	4.60
Period Tracker (Pink Pad)	11246	3819	2252	100	5.0	1.7	22.5	4.60
RunKeeper - GPS Track Run Walk	10819	3607	2186	95	4.9	1.7	23.0	4.46
Sports Tracker	10772	3621	2169	90	5.0	1.7	24.1	4.43
Strava Running and Cycling	10512	3570	2124	116	4.9	1.7	18.3	4.33
Endomondo Sports Tracker	9535	3242	1870	105	5.1	1.7	17.8	3.82
Lose It!	6965	2344	1458	109	4.8	1.6	13.4	2.98
miCoach train & run	6287	2037	1321	89	4.8	1.5	14.8	2.70
Runtastic Running & Fitness	6384	2219	1294	84	4.9	1.7	15.4	2.64
Nike+ Running	6324	2084	1203	64	5.3	1.7	18.8	2.46
Workout Trainer	5278	1777	1064	83	5.0	1.7	12.8	2.17
HealthTap	4574	1527	930	55	4.9	1.6	16.9	1.90
Noom Weight Loss Coach	3114	1032	636	35	4.9	1.6	18.2	1.30

Note that some policies were incorporated in an overall Terms of Service, were linked to a larger corporate privacy policy, or had links to third party privacy policies that were not evaluated in this study. Twelve point Times New Roman font, with an average of 10 words per line and 49 single-spaced lines on a page for a total of 490 words on a single-spaced page was used for determining the average policy length. The comparison of the text statistics for the privacy policies shows an average length of 4.8 pages.

The Flesch-Kincaid Reading Ease (FKRE) Score is based on a 0 to 100 scale, in which the higher the score equates to the text considered easier to read and a lower score suggests that the text is more difficult to understand. A score between 60 and 80 should be easy for a 12 to 15 year old to read. The grade levels for the following scores are approximately representative of the grade levels in the U.S. public schooling system, which should be able to understand the text. The Simple Measure of Gobbledygook (SMOG) Index is considered a substitute for the Gunning Fog Index and was developed in 1969 [28]. SMOG has been successful with assessing the readability of health care related materials [29] and praised for its consistency with health care applications [30]. Note that the formula only works for texts containing more than 30 words and that complex words are considered polysyllabic (i.e., words with three or more syllables). The Coleman-Liau (CL) and the Automated Readability Index (ARI) focus on characters instead of syllables per word. This section presented the readability formulas that were used to evaluate the readability of the privacy policies for the selected health and fitness related mobile applications.

The readability tests by grade level rated the applications in comparable order and the results are presented from lowest to highest FKRE scores (cf. Table 3). The reading grade level averages indicate that many of the privacy policies are written above the 12th grade level. Comparable statistics contributed to the Credit Card Accountability, Responsibility and Disclosure (CARD) Act of 2009 requiring credit card agreements to be written in a common format and at a lower level because many Americans read below the 12th grade level [31]. Similar improvements to end-user comprehension could be made by lowering the readability level required of mobile application privacy policies without changing the integrity of the privacy policies.

Table 3. Comparison of reading tests.

Application	FKRE	FKGL	CL	SMOG	ARI
Daily Workouts FREE	24.3	17.8	15.0	14.7	19.1
iTriage Health	26.1	16.30	16.1	14.9	17.5
Calorie Counter -MyFitnessPal	29	15.5	15.8	13.5	16.4
Weight Watchers Mobile	33.1	14.9	14.4	12.9	15.3
BabyBump Pregnancy Free	40.5	13.2	13.6	12.0	13.4
Period Tracker (Pink Pad)	40.5	13.2	13.6	12.0	13.4
Sports Tracker	41.1	13.5	13.4	12.4	13.9
Nike+ Running	41.2	12.2	15.1	11.3	12.7
Endomondo Sports Tracker	42.1	11.8	14.2	10.7	11.5
My Tracks	42.10	12.30	14.6	11.1	12.8
WebMD for Android	43.5	13.7	12.8	12.1	14.5
RunKeeper - GPS Track Run Walk	43.9	12.9	13.3	11.8	13.4
CVS/pharmacy	44.40	13.40	12.7	12.0	14.2
Runtastic Running & Fitness	46.1	10.7	13.2	9.8	9.5
Strava Running and Cycling	46.1	11.4	13.3	10.5	11.0
HealthTap	50.70	10.30	13.2	9.7	10.1
Noom Weight Loss Coach	51.10	10.60	13.0	10.0	10.7
Workout Trainer	52.5	9.1	13.4	8.7	8.3
Lose It!	57.2	8.6	12.3	8.7	7.8
miCoach train & run	61.3	8.4	12.2	8.0	8.4

3.3 Observations and Recommendations

A diverse set of policies were reviewed which represented small independent developers to multi-national companies, for the purpose of fitness training and health monitoring to pharmacy communication. The quality and complexity widely ranged and the challenge was noticed of creating a single policy in an Internet without borders. There is a lack of uniformity in format, universal language and definitions, which can impact end user comprehension. None of the reviewed applications offered mobile-friendly short forms with links to their full privacy policies. Future regulations should establish standards for language and formats of privacy policies, which could lower end user cognitive loads.

The majority of privacy policies used simple black fonts on white backgrounds with headings in bold text. Hyperlinks were extensively used for company support or contact features, other internal policies (e.g., Security, Terms of Service) and external third-party privacy policies. A few policies offered mouseover tooltip features that offered more detailed information. There was a lack of icon usage, which may supplement rapid comprehension for end users and should be further researched for usability purposes. Only one application (i.e., WebMD) used seals of accreditation within their privacy policies (i.e., URAC, HONcode) to inform end users of their trustworthiness and healthcare quality. URAC , formerly the American HealthCare Accreditation Association, is an independent accrediting body that reviews Web sites for compliance with its more than 45 quality and ethics standards. The Health on the Net (HONcode) rates the reliability and credibility of information on medical and health websites. Future work should investigate the use of trustworthiness seals and end user willingness to share personal information.

The majority of applications (17 out of 20) were maintained by developers based in the U.S., and three were in Europe (Denmark, Austria and Finland). Only a few applications addressed end user procedures for personal data access or correction. It was not possible to determine actual data handling procedures for any countries by their privacy policies, but some multi-national companies most likely have trans-border data flows. In addition, data retention procedures were rarely reported. Only the European countries specifically referred to Data Rights of Access or European Union Directive 95/46/EC. Data sharing procedures and the privacy policies of third parties were usually vague and left up to the end user to determine by following possible hyperlinks. Many policies used statements of indemnity. For example, an ominous warning provided by Daily Workout, “is not liable for the acts and omissions of third parties, except as provided by mandatory law”.

Most policies (14 out of 20) discussed the prohibition of use by minors, but the definitions varied by ages (i.e., 13, 14, 15 and 18 years old). This is the company's prerogative, as long as it supports the Children's Online Privacy Protection Act for applications in the U.S.

3.4 Limitations

A limited sample of popular English health and fitness related mobile applications were examined in this study. Hyperlinks to external third-parties, Terms of Use statements and other company policies were not considered in this survey. A technical study was not conducted to determine if applications were leaking personal information that was not covered in their terms of service or privacy policies. Readability tests have been challenged because they can only measure the surface characteristics of text and do not measure qualitative factors such as: reader interest, sentence composition and structure, impact of graphics, and overall comprehensibility of the examined text.

4. Conclusion

Many privacy policies assessed in this study did not directly address the purpose of collection, transfer, storage and destruction of end-user personal health and fitness information. A major concern is that privacy policies lack a standard format and terminology. Standardized privacy policies would greatly aide end users with comprehension, developers with privacy planning and regulators with compliance inspections. Many policies did not clearly address who exactly they share information (i.e., their affiliates or third-parties), listed procedures for end-users to review their data or used ambiguous language (e.g., "we use a variety of security measures"). This study found that the average privacy policy was written above the 12^{th} grade level and an average length of 4.8 pages. It has been recommended that documents intended for health or safety instructions be written at the 5th grade level and documents for the general public be written at the 9th grade level [25]. Privacy policies that quickly address end-user concerns may become a point of differentiation in the competitive mobile application market. End users may soon increase their demand for health and fitness applications with improved transparency of the data collection procedures.

The FTC has already pursued penalties against developers and businesses that conduct deceptive or unfair business practices (e.g., do not honor their privacy policies). All of the observed mobile applications in the Google Play health and fitness market are unregulated by the FDA. The FDA has stated that it will regulate mobile applications that do the same thing as traditional medical devices [12]. Privacy policies will need to adapt with advances in mobile applications. Remote monitoring and analysis of patients, will open new vectors for security and privacy threats. The trend of mobile applications incorporating end-user motion tracking to conduct activity recognition will also create increased data sets with personally identifiable information.

Software developers may want to consider the concerns of their target end-users and clearly describe how they collect, store and transmit personal information with privacy policies written at an appropriate reading level of their intended end-users. Businesses may want to consider updating their existing privacy policies with lower reading comprehension ratings without compromising the integrity about their commercial data practices dealing with personal information. Lowering readability of privacy policies will allow a larger segment of the end-user population to be able to understand what personal data is being collected and why it is needed. Improved transparency may create an improved trust between service providers and end users that could lead to an increased distribution of their health and fitness software applications. Further investigation is needed in the usability of icons and mobile friendly privacy policies as "short forms" linked to complete information. Future work plans to evaluate a privacy policy generator that provides access to readability test scores to assist novice application developers in creating effective privacy policies.

References

1. Steinberg, J. (2013, December 6). This flashlight android app has been secretly and illegally sharing your personal data with advertisers. Retrieved from: http://www.forbes.com/sites/josephsteinberg/2013/12/06/this-flashlight-android-app-has-been-secretly-and-illegally-sharing-your-personal-data-with-advertisers/.

2. Hoffman, C. (2014, June 11). Android's app permissions were just simplified-now they're much less secure. Retrieved June 11, 2014 from: http://www.howtogeek.com/190863/androids-app-permissions-were-just-simplified-now-theyre-much-less-secure.
3. Conn, J. (2013, July 22). Users beware: leaks from health websites, applications cause for concern. Retrieved June 12, 2014 from: http://www.modernhealthcare.com/article/20130720/MAGAZINE/307209973.
4. Lewis, N. (2011, October 21). 80% of doctors use mobile devices at work. InformationWeek.. Retrieved from: http://www.informationweek.com/80--of-doctors-use-mobile-devices-at-work/d/d-id/1100880.
5. Caldwell, A. (2014, June 30). Apps a 'growing area' in health care, AMA warns doctors still needed. Retrieved June 30, 2014 from: http://mobile.abc.net.au/news/2014-06-30/health-apps-wont-replace-doctor-visits-ama/5559832.
6. Farr, C. (2014, June 5). Wanted: a watchdog for the mobile medical app explosion. Retrieved June 7, 2014 from: http://www.mobilehealthmarketplace.com/.
7. Cox, J. (2014, June 5). Will federal privacy rules afflict apple's new ios healthkit? HIPAA complexities loom for some developers.. Retrieved June 8, 2014 from: http://networkworld.com/article/2360163/wireless/will-federal-privacy-rules-afflict-apple-s-new-ios-healthkit.html.
8. Talbert, R. (2006, July 18). Grim news about reading skill. Retrieved June 7, 2014from: http://chronicle.com/blognetwork/castingoutnines/2006/07/18/grim-news-about-reading-skill/.
9. Institute of Medicine. Health literacy: a prescription to end confusion. April 2004. Retrieved June 30, 2014 from: http://www.iom.edu/Reports/2004/Health-Literacy-A-Prescription-to-End-Confusion.aspx.
10. Federal Trade Commission. (2014). How to keep your personal information secure. Retrieved June 7, 2014, from: http://www.consumer.ftc.gov/articles/0272-how-keep-your-personal-information-secure.
11. Slabodkin, G. (2014, May 8). FTC concerned with health data sharing apps. Retrieved June 10, 2014 from: http://www.healthdatamanagement.com/news/FTC-Concerned-with-Health-Data-Sharing-Apps-48017-1.html.
12. Thompson, B. (2014, June 11). FDA regulation of mobile health. Mobihealth news research. Retrieved June 6, 2014 from: http://mobihealthnews.com/research/fda-regulation-of-mobile-health.
13. U.S. Department of Health & Human Services. (2014). Health information privacy, Summary of the hipaa privacy rule (45 C.F.R. section 106.103). Retrieved June 9, 2014 from: http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html.
14. Ameen, A., Liu, M. and Kwak, K. Security and privacy issues in wireless sensor networks for healthcare applications. *J. Medical Syst.* 2010, 1-9.
15. Giannetsos, T., Dimitriou, T. and Prasad, N. People-centric sensing in assistive healthcare: Privacy challenges and directions. *Security and Communication Network*. 2011, vol. 4, no. 11.
16. Privacy Rights Clearinghouse. (2013, July 15). Mobile health and fitness applications: what are the privacy risks? Retrieved June 9, 2014 from: https://www.privacyrights.org/mobile-medical-applications-privacy-alert%20.
17. McDonald, A. and Cranor, L. The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society*, 2009, vol. 4, no. 3, 543-568.
18. Acquisti, A. and Grossklags, J. An Online Survey Experiment on Ambiguity and Privacy. *Communications & Strategies*, No. 88, 4th Quarter 2012, 19-39. Available at SSRN: http://ssrn.com/abstract=2374342.
19. Graber, M., D'Allessandro, D. and Johnson-West, J. Reading level or privacy policies on internet health web sites. *Journal of Family Practice*. July 2002, vol. 51, no. 7.
20. Meiselwitz, G.. Readability assessment of policies and procedures of social networking sites. In Proceedings of the 5th international conference on Online Communities and Social Computing (OCSC'13), A. Ant Ozok and Panayiotis Zaphiris (Eds.). Springer-Verlag, Berlin, Heidelberg, 67-75.
21. Hoofnagle, C. (2008). What californians understand about privacy online. Samuelson Law, Technology & Public Policy Clinic. Retrieved June 10, 2014 from: http://www.law.berkeley.edu/clinics/samuelsonclinic/files/online_report_final.pdf.
22. Rowan, M. and Dehlinger, J. Privacy incongruity: an analysis of a survey of mobile end-users. 13th International Conference on Security and Management. 2014.
23. Phandroid Forums. (2012, October 31). Confused over app permissions. Retrieved June 11, 2014 from: http://androidforums.com/android-applications/641501-confused-over-app-permissions.html.
24. Google Play. (2014). Review app permissions. Retrieved June 10, 2014 from: https://support.google.com/googleplay/answer/60149727.
25. Dubay, W. (2004, August 25). Principles of readability. Retrieved June 12, 2014 from: http://www.impactinformation.com.
26. Child, D. (2014). Text-Statistics. Retrieved June 11, 2014 from: https://github.com/DaveChild/Text-Statistics.
27. Developer.Android.com, (2014). Security Tips. Retrieved June 11, 2014 from: http://developer.android.com/training/articles/seurity-tips.html.
28. McLaughlin, G. SMOG grading – a new readability formula. *Journal of Reading.* 1989, 12 (8). 639-646.
29. Hedman, A. Using the smog formula to revise a health-related document. *American Journal of Health Education*. 2008. 39 (1). 61-64.
30. Wang, L., Miller, M., Schmitt, M., Wen, F. Assessing readability formula differences with written health information materials: application, results, and recommendations. *Research in Social and Administrative Pharmacy*. 2013, vol. 9. 503-516.
31. Caplinger, D. (2013, October 3). 5 signs that credit card reform is really working. Retrieved June 13, 2014 from: http://www.dailyfinance.com/2013/10/03/credit-card-act-signs-reform-is-working.