Dakota State University

Beadle Scholar

Faculty Research & Publications | College of Business and Information Systems

2022

Privacy and Security Concerns Associated with mHealth Technologies: A Computational Social Science Approach

Mitchell Damion

Omar El-Gayar

Follow this and additional works at: https://scholar.dsu.edu/bispapers

Recommended Citation

Damion, Mitchell and El-Gayar, Omar, "Privacy and Security Concerns Associated with mHealth Technologies: A Computational Social Science Approach" (2022). *Faculty Research & Publications*. 293.
https://scholar.dsu.edu/bispapers/293

This Article is brought to you for free and open access by the College of Business and Information Systems at Beadle Scholar. It has been accepted for inclusion in Faculty Research & Publications by an authorized administrator of Beadle Scholar. For more information, please contact repository@dsu.edu.

Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2022 Proceedings

SIG DSA - Data Science and Analytics for Decision Support

Aug 10th, 12:00 AM

Privacy and Security Concerns Associated with mHealth Technologies: A Computational Social Science Approach

Damion R. Mitchell
Dakota State University, damion.mitchell@trojans.dsu.edu

Omar El-Gayar
Dakota State University, omar.el-gayar@dsu.edu

Follow this and additional works at: https://aisel.aisnet.org/amcis2022

Recommended Citation

Mitchell, Damion R. and El-Gayar, Omar, "Privacy and Security Concerns Associated with mHealth Technologies: A Computational Social Science Approach" (2022). *AMCIS 2022 Proceedings*. 8.
https://aisel.aisnet.org/amcis2022/sig_dsa/sig_dsa/8

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2022 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Privacy and Security Concerns Associated with mHealth Technologies: A Computational Social Science Approach

Completed Research

Damion R. Mitchell
Dakota State University
damion.mitchell@trojans.dsu.edu

Omar El-Gayar
Dakota State University
omar.el-gayar@dsu.edu

Abstract

mHealth technologies seek to improve personal wellness; however, there are still significant privacy and security challenges. The purpose of this study is to analyze tweets through social media mining to understand user-reported concerns associated with mHealth devices. Triangulation was conducted on a representative sample to confirm the results of the topic modeling using manual coding. The results of the emotion analysis showed 67% of the posts were largely associated with anger and fear, while 71% revealed an overall negative sentiment. The findings demonstrate the viability of leveraging computational techniques to understand the social phenomenon in question and confirm concerns such as accessibility of data, lack of data protection, surveillance, misuse of data, and unclear policies. Further, the results extend existing findings by highlighting critical concerns such as users' distrust of these mHealth hosting companies and the inherent lack of data control.

Keywords

mhealth, privacy, security, computational social science, text-mining, ground theory, topic modeling

Introduction

The World Health Organization (WHO) defines mHealth as "*medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants, and other wireless devices*" (World Health Organization 2011). mHealth technologies have transformed the means by which individuals seek and receive healthcare, manage chronic conditions, and access medical records (Acquisti et al. 2015). The global mHealth market is projected to grow at a rate of 36.5% between 2016 and 2022 and would ultimately reach a size of US$ 22.31 billion by the end of 2022 (Market Research Focus 2020). mHealth has emerged over the past 20 years as an integrative discipline, focusing on developing and implementing wireless, portable, or implantable technology for improving human health (Andreu-Perez et al. 2015). With the advent of miniaturized sensors, low-power body-area wireless networks, and pervasive smartphones, the burgeoning field of mHealth technologies have attracted tremendous commercial activity, consumer interest, and adoption by major healthcare providers (Kotz et al. 2016). mHealth sensing devices can help individuals work towards a healthier lifestyle or allow them to share the collected information with their doctor to diagnose health issues or manage a chronic disease (Prasad et al. 2012).

Although mHealth technologies may indeed improve quality of healthcare and quality of life, they also generate security and privacy issues. Past research has focused on privacy and security concerns in the context of mHealth technologies (Arora et al. 2014; Zhao et al. 2020). The privacy and security of personal data while using mHealth devices continue to be of great concern. Other research have examined different health related issues through the use of social media mining (Correia et al. 2020; Domalewska 2021). However, with social networking sites serving as lens through which public sentiments and perspectives can be easily accessed, little has been done to investigate the privacy and security concerns of users, associated with mHealth technologies, through social media mining.

In this research paper, we investigate the various privacy and security concerns expressed by social media users in relation to the use of mHealth technologies, using a computational social science approach. The study seeks to answer the following research questions:

- **RQ1:** What are the privacy and security concerns associated with mHealth technologies?
- **RQ2:** What is the general sentiment towards mHealth privacy and security related issues?
- **RQ3:** How has the perception of various mHealth related issues evolved over time?

Related Work

Extant literature commonly cited privacy problems as primary barrier to the persistent adoption of mHealth technologies such as wearables (Kang et al. 2013; Lee et al. 2015). Previous research has shown that privacy concerns and perceptions of security risks can hinder the usage of e-commerce systems (Eastlick et al. 2006), online health information systems (Bansal et al. 2010) and in particular location-based services (LBS) of mHealth technologies (Zhou 2012). The concept of privacy is not new, and it has generally been defined as an individual's ability to control the terms by which their personal information is acquired and used (Westin 1968). It was posited by Bunnig and Cap (2009) that privacy involves protecting personal information from being misused by malicious entities and allowing certain authorized entities to access that personal information by making it visible to them.

Privacy and security issues impede the adoption and diffusion of technology in the IT domain (Cho et al. 2009; Lee et al. 2011). Owing to the high data sensitivity and the mobility of the devices, privacy concerns have proved to be more important in the context of health wearables than other technological devices (Miltgen et al. 2013). It was posited that privacy-related threats can be classified as identity threats, where patients may lose their identity credentials, thus allowing access to their personal health information (PHI); and access threats, where patients have ultimate control on the collection, use, and disclosure of PHI, but if they fail to express their consent broader-than-intended access may be granted (Plachkinova et al. 2015). Security refers to the safeguards, techniques, and tools used to protect against the inappropriate access or disclosure of information. As such it is one of the key factors in protecting the users from any type of uncertainties and risks. In the mHealth context specifically, security covers the triads of confidentiality (ensuring that the collected data is accessible only to the authorized entities), integrity (ensuring the correctness and trueness of the data being transmitted), and availability (survivability despite security attacks). Users' security concerns are a serious issue that can affect the trust levels and hinder the adoption rate (AlHogail 2018; Falcone and Sapienza 2018). Therefore, mHealth technologies such as wearables must gain the users' confidence and provide assurance that they will be safe.

Research Methodology

Figure 1 shows the research methodology adopted in this study. According to Al-Ramahi et al. (2016), text mining and grounded theory are seen as epistemologically compatible since text mining allows for the extraction of concepts and theories from the data. Therefore, we sought to automate the extraction and analysis of social media posts through text mining within the grounded theory framework (Charmaz 2006). The first stage involved data collection, based on a specific time and keywords of interest. The collected tweets were pre-processed and open-coded using text mining. The Latent Dirichlet Allocation (LDA) algorithm was used for topic modeling to automatically extract concepts from the large corpus of text data. These findings were then confirmed using manual coding through ATLAS.ti on a representative sample. We performed axial coding and selective coding to extract relevant higher-level categories and propositions. Brandwatch (BW), a social media mining platform was used to analyze the data for aspects such as sentiment and trend analyses.

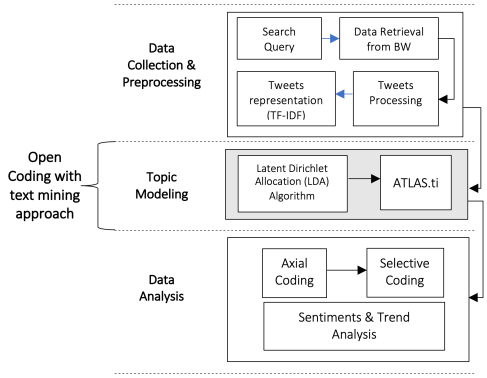

Figure 1. Research Approach (Adapted from Al-Ramahi et al. 2016)

Data Collection and Preprocessing

Our target social media platform for data collection was the microblogging platform Twitter. We used Brandwatch which provides access to the "Twitter firehose" to extract English tweets for the period June 1, 2010, to December 31, 2021. The keywords such as intrusion, theft, surveillance, expose, tracking, or data control were identified by examining the literature (Motti and Caine 2014; Solove 2006) as well as using online synonym generators. The collected tweets were pre-processed by removing stop words, retweets, addresses, and certain words that are not context appropriate. We performed lemmatization and represented each document using the well-known Term Frequency Inverse Document Frequency (TF-IDF) weighting scheme (Haddi et al. 2013).

Open Coding using text mining

There are generally three analytic types of coding in grounded theory, namely: open coding, axial coding, and selective coding. Open coding comes up with concepts, while axial coding represents the process of developing main categories and their sub-categories. Lastly, selective coding deals with the integration of the categories that have been developed to build theoretical framework (Pandit 1996). Data analysis is a fundamental component in grounded theory, since theories are developed from the data (Corbin and Strauss 1990). In this phase of the analysis the labeling and categorization of the phenomena discovered in the posts was done (Charmaz 2006). Text mining is a process of obtaining useful information from document collections through the identification and exploration of interesting patterns (Feldman and Sanger 2006). The text-mining process like that of grounded theory requires impartiality which will allow for categories to emerge from the data (Yu et al. 2011). The researchers sought to apply text mining techniques to facilitate the coding of social media posts, with further analysis done using grounded theory to improve the quality of the concepts and categories which were used in the analysis.

Topic models are statistical algorithms that can be used to discover the hidden thematic structure (i.e., topics) from large unstructured collections of documents by analyzing the words within the texts (Blei 2012). Topic modeling algorithms do not necessitate any prior labeling or annotations of the documents and allow the topics to emerge from the examination of the original texts. In this study, LDA-based topic Modeling (Blei 2003) was used, which is known to have the highest performance among several topic modeling algorithms when dealing with large-scale documents and interpreting identified latent topics (Chiru et al. 2014). The model produces automatic summaries of topics in terms of a discrete probability distribution over words for each topic, additionally it deduces per-document discrete distributions over topics.

The interface between the observed documents and hidden topic structure is revealed in the probabilistic generative process associated with LDA (Blei 2012). LDA assumes the following generative process for a corpus D consisting of M documents which were extracted from Brandwatch, each of length N_i. To demonstrate the results of LDA, Let M be the number of documents in a collection, K the number of topics, N the number of words in a document, *and* V the vocabulary size. The first result is the $M \times K$ matrix, where the weight $w_{m,k}$ is the relationship between a document d_m and a topic t_k. The second result is the $N \times K$ matrix, where the weight $w_{n,k}$ is the connection between a word w_n and a topic t_k. LDA-based topic modeling

is a useful technique for latent topic identification from a large corpus; the study used it to identify security and privacy concerns in mHealth Technologies discussed by users in social media. Topics are typically manually labeled to ensure high labeling quality, particularly when such classification requires domain knowledge (Chang et al. 2009). To guarantee that the labeling was not biased, two independent researchers reviewed and labeled the 10 topics generated by the LDA model.

Axial & Selective Coding

We performed axial coding which involved the development of main categories and their sub-categories (Charmaz 2006). In grounded theory, selective coding refers to the incorporation of the categories that have been discovered during the axial coding to form the theoretical framework (Pandit 1996). These were grouped based on a privacy taxonomy (Solove 2006) and formed the basis for the analysis of the data.

Sentiments & Trend Analysis

Textual data can be broadly categorized into facts and opinions; facts are objective expressions such as entities and events and their properties, while opinions are subjective expressions that describe people's sentiments, appraisals, or feelings (Liu 2010). Sentiment analysis involves the task of automatically ascribing positive, negative, or neutral sentiment to portions of text that express opinions (Jeong et al. 2019). Furthermore, emotion analysis provides an additional layer of contextual analysis by the utilization of "Ekman 6" (Anger, Fear, Disgust, Joy, Surprise, and Sadness) basic human emotions (Ekman 1993). The researchers used Brandwatch which employs BrightView, a supervised algorithm that is an updated version of the ReadMe algorithm developed by (Hopkins and King 2010). The algorithm is based on aggregate analysis to allow flexibility and accuracy, which is primarily suited when the researcher wants to depict the volume of tweets that fit in to specific categories over time. The algorithm requires the researcher to manually code a training set of documents into a set of predefined groups. In contrast to traditional classification methods that focus on maximizing the percent of documents correctly classified into a given set of categories, the ReadMe algorithm emphasizes the broad categorization about the whole sets of documents (Hopkins & King, 2010). Accordingly individual-level classification is not a result of this method and traditional classification performance metrics based on the confusion matrix do not apply. Examples further illustrating the use of the algorithm and its supporting platform include Al-Ramahi et al. (2021), El-Gayar et al. (2021), Jamal et al. (2015), Kim et al. (2013), and Runge et al. (2013). In this study, the collected tweets represent the set of documents, and the predefined categories were obtained from the topic modeling stage. The researcher assigned at least 20 tweets into each category, after which the BrightView algorithm was executed on past and future tweets returned by the search query. The tweets were examined based on the assigned categories, and further training was conducted where necessary.

Results

The query resulted in a total of 25,525 English tweets for the designated period (figure 2).

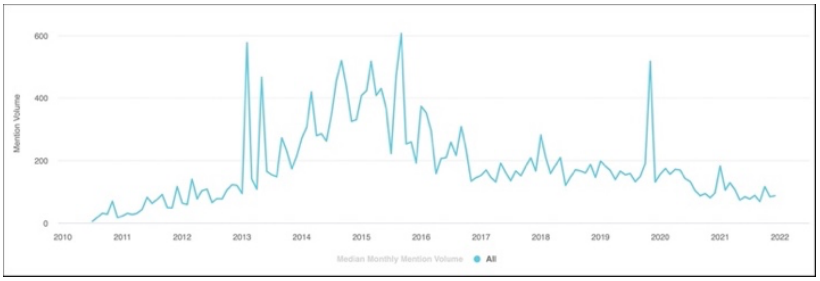

Figure 2. Volume of Tweets for Search Period

Privacy and security concerns of social media users in the context of mHealth technologies

In response to research question 1, Figure 3 highlights four sample word clouds of the result of a 10-topic LDA model produced during the open coding phase, where each topic was represented by the top-15

weighted words in its vocabulary distribution. An illustrative word or phrase was then assigned to each topic to signify the main privacy and security concerns related to mHealth technologies. Table 2 shows the evidence from the data about each privacy and security concern.

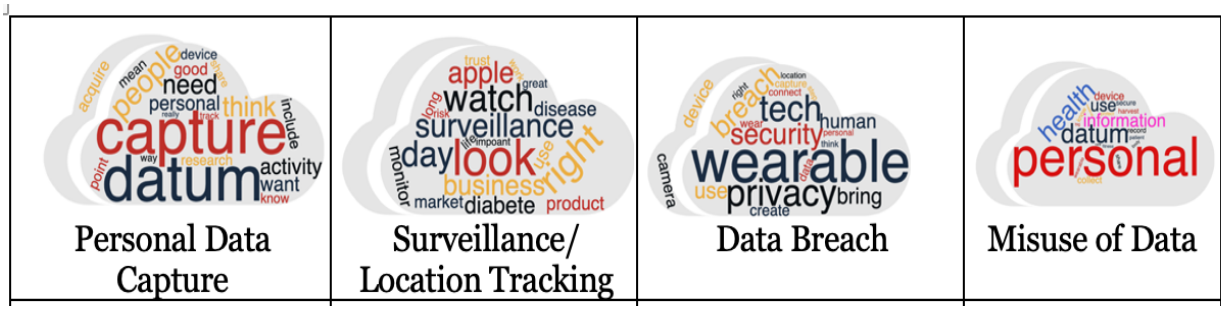

Figure 3. Sample Word Clouds of the LDA Topic Model

Based on the ten privacy and security concerns discovered from the open coding stage, the concepts were then grouped during the axial and selective coding phases into four privacy theoretical dimensions, namely: information collection, information processing, information dissemination and data invasion as shown in Figure 4. In the area of information collection surveillance concern arises when the personal information and social interactions of OSN users are leveraged by governments and service providers (Gurses and Diaz 2013). Furthermore, mHealth devices capture large amounts of personal data based on their capacity for continuous data recording at high frequencies (Wu and Luo 2019). As an example, the issue of *"personal data capture"* and *"surveillance/location tracking"* of mHealth users were generalized and placed as information collection (Hann et al. 2007).

Privacy and Security Concerns	Example Tweets
Surveillance / Location Tracking	I have opted out of sharing my activity data, but perhaps there's a shared tracking cookie that could be leaking my location
Personal Data Capture	Many wearable devices seem to be connected to applications that capture data that people could use to monitor aspects of your daily life.
Misuse of Data	@fitbit so I've heard you have just sold all my health personal and sensitive data to... who could never ever have access to it... Google! Fitbit just showing their commitment in (not) respecting my personal data. pls let me know if I can opt out
Distrust of Company	@GoogleHealth How do we get our Personal data from the Fitbit Buyout so it's only available to us & deleted From Google Servers?
Data Control	When your government seeks to control your life through biometric wearables, it might be time to opt-out.
Accessibility of Data	When I click on Privacy policy, it returns to the main page! A bit unclear who will access and manage the personal data!
Data Breach	Wearables present several opportunities for a data breach. Most are relatively easy to a hack a wearable with password-fingerprint ID security.
Unclear/Lack of Policies	Fitbit just bought by google - prepare for all your personal data to be mined and distributed/sold as they see fit. The amended data agreement should be winging its way to you now.
Data Theft	Fitbit Spyware Steals Personal Data via Watch Face. #Fitbit #Security #Spyware
Data Protection	So, @fitbit, do you now encrypt both your storage and transmission of the personal data created? Your earlier models didn't...just asking for #privacy and #cybersecurity reasons

Table 2. Privacy and Security Concerns with Evidence from the Data

In addition, the *"misuse of data"* not only by the companies of these mHealth devices but third-party applications along with the *"distrust of the company"* in terms of the how collected data were being treated were grouped as information processing (Rath and Kumar 2021). This occurs when providers collect private and sensitive data which can be misused by data collectors, third parties, or by unauthorized users (Ali et al. 2018). The privacy and security concerns such as *"data control", "accessibility of data", "data breach"* and *"unclear user policies"* were grouped under the area of information dissemination (Baruh et al. 2017). Finally, *"data theft"* and *"lack of data protection"* all related to data invasions (Smith and Milberg 1996). Figure 3 also shows that users had challenges with either unclear/lack of policies under key areas such as information collection, processing, and dissemination.

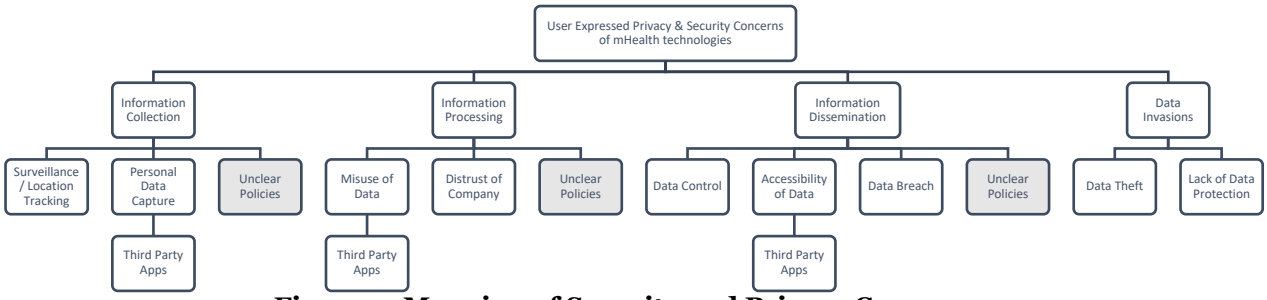

Figure 4. Mapping of Security and Privacy Concerns

Sentiment towards mHealth privacy and security related issues

Figure 5 summarizes the results of the emotion and sentiment analyses based on the collected tweets. The emotion analysis results show that 67% of the posts were reflecting anger and fear, which highlights users' mindset against the privacy and security concerns of mHealth technologies. For example, *"All of your location and fitness data just got acquired by the world's largest surveillance company and there's nothing you can do about it. How do you feel about breaking up some of these companies now?"* The Sentiment analysis shows that 71% of the posts were classified as a negative sentiment, however, 29% were positive, indicating that users are ambivalent towards privacy and security concerns, despite mentions of privacy or security in their posts, there was a general positive tone.

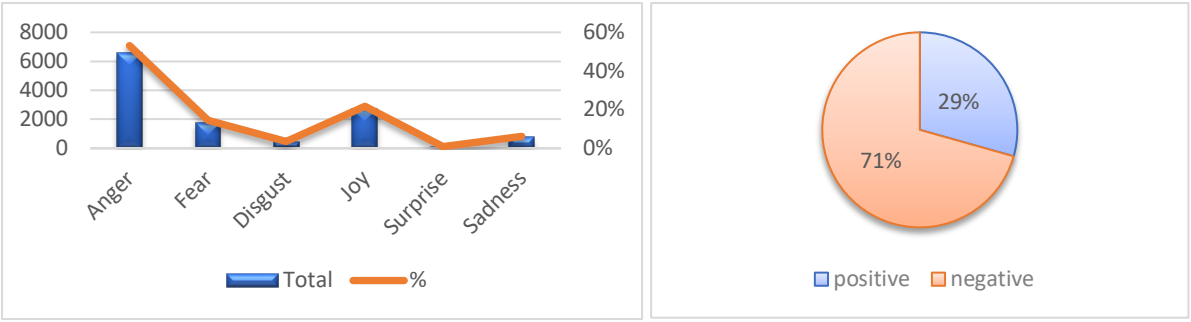

Figure 5. Emotion and Sentiment Analyses

Perception of various mHealth related issues evolved over time

Overall, results show that posts that discussed the concerns of accessibility of data account for 23% of the total posts, followed by lack of data protection, 20%, then surveillance, 18%, misuse of data, 11%, and unclear/lack of policies, 10%. The remaining privacy and security concerns were discussed in less than 10% of the related posts. In addition, Figure 6 shows the volume of tweets over time by category. The period 2013 to 2017 had several posts being made especially in concerned areas of surveillance, lack of data protection, and the accessibility of data.

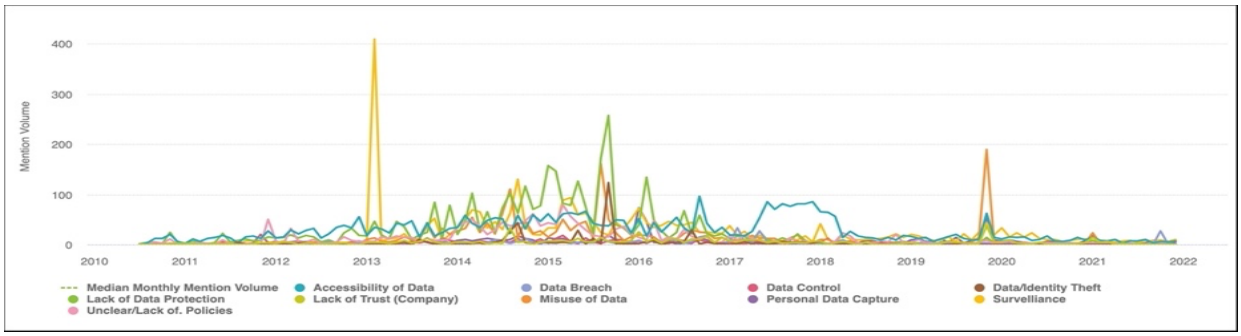

Figure 6. Posts Based on Different Categories

Discussion

The comparison in Table 3 depicts previous studies that examined the privacy and security concerns in various domains. For example, Arora et al. (2014) found that surveillance, data control, accessibility of data and data breach constituted some of the main concerns in mHealth. A privacy framework was developed by Kotz et al. (2009) which covered five (5) of the ten concerns discovered from the data, these include: data capture, data protection, data control, accessibility of data, and data theft. The study presented by Jusob et al. (2022), also confirms our findings with empirical support for six (6) of the concerns outlined. In a study examining the privacy concerns in wearable devices, Datta et al. (2018) demonstrated the concerns surrounding surveillance, unclear policies, distrust of company, data control. Based on the comparison it shows that users are mostly concerned about surveillance, data control and accessibility of data.

Overall, the findings showed that social media could help to identify important insights related to privacy and security concerns, specifically with mHealth technologies. The period 2013 to 2017 saw a flurry of discussions about varying privacy and security concerns. There were many activities around 2015, which could be due to the increase download of fitness applications (Krebs and Duncan 2015). Furthermore, another detected peak in 2020 in the surveillance domain, could be attributed to the acquisition of Fitbit by Google at the end of 2019. The sentiment and emotion analysis results showed that the collected tweets were largely associated with anger and fear, and an overall negative experience. The study demonstrated the potential of social media analytics for reporting privacy and security concerns of users of mHealth technologies. These analytics can certainly inform developers of mHealth technologies of the perceived concerns of these users. In addition, it can help policy makers with developing comprehensive policies to govern data collection, dissemination, and processing on these devices.

	Information Collection			**Information Processing**			**Information Dissemination**				**Data Invasion**	
Study	**Surveillance**	**Data Capture**	**Unclear Policies**	**Misuse of Data**	**Distrust of Company**	**Unclear Policies**	**Data Control**	**Accessibility of Data**	**Data Breach**	**Unclear Policies**	**Data Theft**	**Data Protection**
Arora et al. (2014)	*						*	*	*			
Kotz et al. (2009)		*					*	*			*	*
Jusob et al. (2022)	*			*			*	*			*	*
Datta et al. (2018)	*		*		*	*	*			*		

Table 3. Comparison with Existing Literature

Pertaining to the evaluation of the grounded theory research results, two fundamental criteria should be assessed (Myers 2009). Firstly, the rigor and validity of the qualitative data analysis must be assessed. In this study the rigor of the content analysis was accomplished using a text mining technique which allowed for the extraction of primitive concepts from large volume of text data. It was posited by Yu et al. (2011) that a higher degree of consistency and reliability can be comprehended through the extraction of knowledge from a sizable volume of data compared to manual coding with limited occurrences of the data. Furthermore, multiple instances of posts were highlighted which supported the privacy and security concerns extrapolated. Secondly, the generalization of the research is another key criterion (Myers 2009) The researchers confirmed four important aspects of privacy and security concerns of mHealth users: information collection, processing, dissemination, and data invasion.

Conclusion

The purpose of this study was to analyze tweets through social media mining to understand the user-reported privacy and security concerns associated with mHealth devices. The study adopts a computational science approach where it leverages the capability of text mining within the context of grounded theory. The LDA algorithm for topic modeling was used to automatically analyze the content of the collected tweets. For triangulation purposes, ATLAS.ti was used to manually code a representative sample of the posts collected to confirm the findings. The results showed several privacy and security concerns which are being discussed

on social media to include: lack of data protection, data breach, data control, surveillance/location tracking, misuse of data, etc. Theoretically, the findings provide evidence that information collection, processing, and dissemination are all affected by unclear/lack of policies. Further, distrust of company is likely to influence the acceptance of these technologies, therefore the results also contribute to the literature of users' acceptance of health consumer technology. Practically, these findings can assist policy makers, system developers, and manufacturers of these devices, with a clearer understanding of the expressed privacy and security concerns. Furthermore, found data available on the Web provides opportunities for tracking and analyzing actual users' opinions about a phenomenon, such as wearable devices, and can provide better indicators of such devices' acceptance and use (Motiwalla et al. 2019). A limitation of the study is the potential noise that accompany social media posts and the impact of pulling data from only one social media platform, which could impact the findings. Therefore, a survey study will be conducted to further explore the generalizability of these findings. In addition, understanding the concerns from users on other popular social media platforms like Reddit and Facebook may be beneficial. Future research may investigate other factors relating to privacy and security concerns in mHealth usage and adoption such as the role of age, gender, and culture. Further studies will examine the relationships that exist between expressed sentiments and each privacy and security concerns. Also, we aim to expand the selective coding phase in the grounded theory approach to develop an emergent theory that explains the concerns of these users.

REFERENCES

Acquisti, A., Brandimarte, L., and Loewenstein, G. 2015. "Privacy and Human Behavior in the Age of Information," *Science* (347:6221), pp. 509–514. (https://doi.org/10.1126/science.aaa1465).

AlHogail, A. 2018. "Improving IoT Technology Adoption through Improving Consumer Trust," *Technologies* (6:3), Multidisciplinary Digital Publishing Institute, p. 64. (https://doi.org/10.3390/technologies6030064).

Ali, S., Islam, N., Rauf, A., Din, I., Guizani, M., and Rodrigues, J. 2018. "Privacy and Security Issues in Online Social Networks," *Future Internet* (10:12), p. 114. (https://doi.org/10.3390/fi10120114).

Al-Ramahi, M., El-Gayar, O., and Liu, J. 2016. "Discovering Design Principles for Persuasive Systems: A Grounded Theory and Text Mining Approach," in *2016 49th Hawaii International Conference on System Sciences (HICSS)*, Koloa, HI, USA: IEEE, January, pp. 3074–3083. (https://doi.org/10.1109/HICSS.2016.387).

Al-Ramahi, M., Elnoshokaty, A., El-Gayar, O., Nasralah, T., and Wahbeh, A. 2021. "Public Discourse Against Masks in the COVID-19 Era: Infodemiology Study of Twitter Data," *JMIR Public Health and Surveillance* (7:4), p. e26780. (https://doi.org/10.2196/26780).

Andreu-Perez, J., Leff, D., Ip, H., and Yang, G.-Z. 2015. "From Wearable Sensors to Smart Implants-–Toward Pervasive and Personalized Healthcare," *IEEE Transactions on Bio-Medical Engineering* (62). (https://doi.org/10.1109/TBME.2015.2422751).

Arora, S., Yttri, J., and Nilsen, W. 2014. "Privacy and Security in Mobile Health (MHealth) Research," *Alcohol Research : Current Reviews* (36:1), pp. 143–151.

Bansal, G., Zahedi, F. "Mariam," and Gefen, D. 2010. "The Impact of Personal Dispositions on Information Sensitivity, Privacy Concern and Trust in Disclosing Health Information Online," *Decision Support Systems* (49:2), pp. 138–150. (https://doi.org/10.1016/j.dss.2010.01.010).

Baruh, L., Secinti, E., and Cemalcilar, Z. 2017. "Online Privacy Concerns and Privacy Management: A Meta-Analytical Review: Privacy Concerns Meta-Analysis," *Journal of Communication* (67). (https://doi.org/10.1111/jcom.12276).

Blei, D. M. 2003. *Latent Dirichlet Allocation*, p. 30.

Blei, D. M. 2012. "Probabilistic Topic Models," *Communications of the ACM* (55:4), pp. 77–84. (https://doi.org/10.1145/2133806.2133826).

Bunnig, C., and Cap, C. H. 2009. "Ad Hoc Privacy Management in Ubiquitous Computing Environments," in *2009 Second International Conference on Advances in Human-Oriented and Personalized Mechanisms, Technologies, and Services*, September, pp. 85–90. (https://doi.org/10.1109/CENTRIC.2009.20).

Chang, J., Boyd-Graber, J., Gerrish, S., Wang, C., and Blei, D. M. 2009. *Reading Tea Leaves: How Humans Interpret Topic Models*, p. 10.

Charmaz, K. 2006. *Constructing Grounded Theory*, London; Thousand Oaks, Calif: Sage Publications.

Chiru, C., Rebedea, T., and Ciotec, S. 2014. "Comparison between LSA-LDA-Lexical Chains," *WEBIST 2014 - Proceedings of the 10th International Conference on Web Information Systems and Technologies* (Vol. 2).

Cho, H., Rivera, M., and Lim, S. S. 2009. "A Multinational Study on Online Privacy: Global Concerns and Local Responses," *New Media & Society - NEW MEDIA SOC* (11), pp. 395–416. (https://doi.org/10.1177/1461444808101618).

Corbin, J., and Strauss, A. 1990. *Grounded Theory Research: Procedures, Canons, and Evaluative Criteria*, p. 19.

Correia, R., Wood, I., Bollen, J., and Rocha, L. 2020. *Mining Social Media Data for Biomedical Signals and Health-Related Behavior*.

Datta, P., Namin, A. S., and Chatterjee, M. 2018. "A Survey of Privacy Concerns in Wearable Devices," in *2018 IEEE International Conference on Big Data (Big Data)*, Seattle, WA, USA: IEEE, December, pp. 4549–4553. (https://doi.org/10.1109/BigData.2018.8622110).

Domalewska, D. 2021. "An Analysis of COVID-19 Economic Measures and Attitudes: Evidence from Social Media Mining," *Journal of Big Data* (8). (https://doi.org/10.1186/s40537-021-00431-z).

Eastlick, M. A., Lotz, S. L., and Warrington, P. 2006. "Understanding Online B-to-C Relationships: An Integrated Model of Privacy Concerns, Trust, and Commitment," *Journal of Business Research* (59:8), pp. 877–886. (https://doi.org/10.1016/j.jbusres.2006.02.006).

Ekman, P. 1993. "Facial Expression and Emotion," *American Psychologist* (48:4), US: American Psychological Association, pp. 384–392. (https://doi.org/10.1037/0003-066X.48.4.384).

El-Gayar, O., Wahbeh, A., Nasralah, T., Noshokaty, A. E., and Al-Ramahi, M. A. 2021. "Mental Health and the COVID-19 Pandemic: Analysis of Twitter Discourse," in *Twenty-Seventh Americas Conference on Information Systems*, p. 11.

Falcone, R., and Sapienza, A. 2018. "On the Users' Acceptance of IoT Systems: A Theoretical Approach," *Information* (9:3), Multidisciplinary Digital Publishing Institute, p. 53. (https://doi.org/10.3390/info9030053).

Feldman, R., and Sanger, J. 2006. *The Text Mining Handbook: Advanced Approaches in Analyzing Unstructured Data*, Cambridge: Cambridge University Press. (https://doi.org/10.1017/CBO9780511546914).

Gurses, S., and Diaz, C. 2013. "Two Tales of Privacy in Online Social Networks," *Security & Privacy, IEEE* (11), pp. 29–37. (https://doi.org/10.1109/MSP.2013.47).

Haddi, E., Liu, X., and Shi, Y. 2013. "The Role of Text Pre-Processing in Sentiment Analysis," *Procedia Computer Science* (17), pp. 26–32. (https://doi.org/10.1016/j.procs.2013.05.005).

Hann, I.-H., Hui, K.-L., Lee, S.-Y. T., and Png, I. P. L. 2007. "Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach," *Journal of Management Information Systems* (24:2), Taylor & Francis, Ltd., pp. 13–42.

Hopkins, D. J., and King, G. 2010. "A Method of Automated Nonparametric Content Analysis for Social Science," *American Journal of Political Science* (54:1), pp. 229–247. (https://doi.org/10.1111/j.1540-5907.2009.00428.x).

Jamal, A. A., Keohane, R. O., Romney, D., and Tingley, D. 2015. "Anti-Americanism and Anti-Interventionism in Arabic Twitter Discourses," *Perspectives on Politics* (13:1), Cambridge University Press, pp. 55–73. (https://doi.org/10.1017/S1537592714003132).

Jeong, B., Yoon, J., and Lee, J.-M. 2019. "Social Media Mining for Product Planning: A Product Opportunity Mining Approach Based on Topic Modeling and Sentiment Analysis," *International Journal of Information Management* (48), pp. 280–290. (https://doi.org/10.1016/j.ijinfomgt.2017.09.009).

Jusob, F. R., George, C., and Mapp, G. 2022. "A New Privacy Framework for the Management of Chronic Diseases via MHealth in a Post-Covid-19 World," *Journal of Public Health* (30:1), pp. 37–47. (https://doi.org/10.1007/s10389-021-01608-9).

Kang, K., Pang, Z., and Wang, C. 2013. "Security and Privacy Mechanism for Health Internet of Things," *The Journal of China Universities of Posts and Telecommunications* (20), pp. 64–68. (https://doi.org/10.1016/S1005-8885(13)60219-8).

Kim, A. E., Hansen, H. M., Murphy, J., Richards, A. K., Duke, J., and Allen, J. A. 2013. "Methodological Considerations in Analyzing Twitter Data," *Journal of the National Cancer Institute. Monographs* (2013:47), pp. 140–146. (https://doi.org/10.1093/jncimonographs/lgt026).

Kotz, D., Avancha, S., and Baxi, A. 2009. "A Privacy Framework for Mobile Health and Home-Care Systems," in *Proceedings of the First ACM Workshop on Security and Privacy in Medical and Home-Care Systems - SPIMACS '09*, Chicago, Illinois, USA: ACM Press, p. 1. (https://doi.org/10.1145/1655084.1655086).

Kotz, D., Gunter, C. A., Kumar, S., and Weiner, J. P. 2016. "Privacy and Security in Mobile Health: A Research Agenda," *Computer* (49:6), pp. 22–30. (https://doi.org/10.1109/MC.2016.185).

Krebs, P., and Duncan, D. T. 2015. "Health App Use Among US Mobile Phone Owners: A National Survey," *JMIR MHealth and UHealth* (3:4), p. e4924. (https://doi.org/10.2196/mhealth.4924).

Lee, C., Eze, U., and Ndubisi, N. 2011. "Analyzing Key Determinants of Online Repurchase Intentions," *Asia Pacific Journal of Marketing and Logistics* (23), pp. 200–221. (https://doi.org/10.1108/13555851111120498).

Lee, L., Egelman, S., Lee, J. H., and Wagner, D. 2015. "Risk Perceptions for Wearable Devices," *ArXiv:1504.05694 [Cs]*. (http://arxiv.org/abs/1504.05694).

Liu, B. 2010. *Sentiment Analysis and Subjectivity*, p. 38.

Market Research Focus. 2020. "Mhealth Market Size, Share, Trends, Growth, Analysis-2027." (https://www.marketresearchfuture.com/reports/mobile-health-market-1816, accessed June 21, 2021).

Miltgen, C., Popovič, A., and Oliveira, T. 2013. "Determinants of End-User Acceptance of Biometrics: Integrating the 'Big 3' of Technology Acceptance with Privacy Context," *Decision Support Systems* (56), pp. 103–114. (https://doi.org/10.1016/j.dss.2013.05.010).

Motiwalla, L., Deokar, A. V., Sarnikar, S., and Dimoka, A. 2019. "Leveraging Data Analytics for Behavioral Research," *Information Systems Frontiers* (21:4), pp. 735–742. (https://doi.org/10.1007/s10796-019-09928-8).

Motti, V. G., and Caine, K. 2014. "Human Factors Considerations in the Design of Wearable Devices," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (58:1), SAGE Publications Inc, pp. 1820–1824. (https://doi.org/10.1177/1541931214581381).

Myers, M. D. 2009. *Qualitative Research in Business & Management*, Qualitative Research in Business & Management, Thousand Oaks, CA: Sage Publications Ltd, pp. xii, 284.

Pandit, N. R. 1996. *The Creation of Theory: A Recent Application of the Grounded Theory Method*. (https://doi.org/10.46743/2160-3715/1996.2054).

Plachkinova, M., Andrés, S., and Chatterjee, S. 2015. "A Taxonomy of MHealth Apps – Security and Privacy Concerns," in *2015 48th Hawaii International Conference on System Sciences*,, January, pp. 3187–3196. (https://doi.org/10.1109/HICSS.2015.385).

Prasad, A., Sorber, J., Stablein, T., Anthony, D., and Kotz, D. 2012. "Understanding Sharing Preferences and Behavior for MHealth Devices," in *Proceedings of the 2012 ACM Workshop on Privacy in the Electronic Society*, WPES '12, New York, NY, USA: Association for Computing Machinery, October 15, pp. 117–128. (https://doi.org/10.1145/2381966.2381983).

Rath, D. K., and Kumar, A. 2021. "Information Privacy Concern at Individual, Group, Organization and Societal Level - a Literature Review," *Vilakshan - XIMB Journal of Management* (18:2), Emerald Publishing Limited, pp. 171–186. (https://doi.org/10.1108/XJM-08-2020-0096).

Runge, K. K., Yeo, S. K., Cacciatore, M., Scheufele, D. A., Brossard, D., Xenos, M., Anderson, A., Choi, D., Kim, J., Li, N., Liang, X., Stubbings, M., and Su, L. Y.-F. 2013. "Tweeting Nano: How Public Discourses about Nanotechnology Develop in Social Media Environments," *Journal of Nanoparticle Research* (15:1). (https://doi.org/10.1007/s11051-012-1381-8).

Smith, H. J., and Milberg, S. J. 1996. "Information Privacy: Measuring Individuals' Concerns about Organizational Practices," *MIS Quarterly* (20:2), pp. 167–196. (https://doi.org/10.2307/249477).

Solove, D. J. 2006. "A Taxonomy of Privacy," *University of Pennsylvania Law Review* (154:3), p. 477. (https://doi.org/10.2307/40041279).

Westin, A. 1968. "Privacy And Freedom," *Washington and Lee Law Review* (25:1), p. 166.

World Health Organization. 2011. *MHealth: New Horizons for Health through Mobile Technologies: Second Global Survey on EHealth*, World Health Organization. (https://www.cabdirect.org/globalhealth/abstract/20113217175).

Wu, M., and Luo, J. 2019. "Wearable Technology Applications in Healthcare: A Literature Review." (https://www.himss.org/resources/wearable-technology-applications-healthcare-literature-review, accessed February 17, 2022).

Yu, C. H., Jannasch-Pennell, A., and Digangi, S. 2011. "Compatibility between Text Mining and Qualitative Research in the Perspectives of Grounded Theory, Content Analysis, and Reliability," *Qualitative Report* (16), pp. 730–744. (https://doi.org/10.46743/2160-3715/2011.1085).

Zhao, W., Shahriar, H., Clincy, V., and Bhuiyan, Z. A. 2020. "Security and Privacy Analysis of Mhealth Application: A Case Study," in *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, December, pp. 1882–1887. (https://doi.org/10.1109/TrustCom50675.2020.00257).

Zhou, T. 2012. "Examining Location-Based Services Usage From The Perspectives Of Unified Theory Of Acceptance And Use Of Technology And Privacy Risk," *Journal of Electronic Commerce Research* (13:2), p. 10.