4-21-2017

Permissions between Creators and Users: An Investigation of Particulars in Privacy Policies for Mobile Apps

Abbigail Griffith
Western Michigan University, abbiegriffith1018@gmail.com

Permissions Between Creators and Users: An Investigation of Particulars in Privacy Policies for Mobile Apps

Abbigail Griffith

The Lee Honors College at Western Michigan University

Table of Contents

Abstract
Mobile apps create a space for users to share information with other users and, in doing so, the creators of the applications. Generally, the greater amount of sharing information that occurs between users and creators enhances the experience of the apps for both parties. However, the extent to which mobile apps use this information can cause concerns with users about privacy due to the unknown practices of mobile apps relevant to data collection, data sharing, and data storage.

Documents, such as privacy policies, exist in attempts to moderate these concerns. Additionally, mobile apps offer in-app features for the same reasons. Previous work does not develop a connection between policy language and in-app features, called control mechanisms, to address these interests of privacy; and if policy language or control mechanisms address these interests more than the other. This study considers four mobile apps, all categorized as social networking apps, to evaluate how policy language and control mechanisms meet users' privacy concerns, and which favors control on behalf of the user or the creator.

Analysis of the documents titled, "Privacy Policies," or, "Data Policy," revealed that privacy policy language benefits the creators of mobile apps; while in-app features more so service users of mobile apps. In-app features respects users by offering more control in managing privacy concerns. There continues to be constant negotiation in the relationship between creators and users; neither entity wants to give up more advantages than necessary. Limitations and future implications resolve this study.

Introduction

Privacy is a sensitive topic across mediums. In particular, online privacy is an inherently ambiguous item due to the vast operations of the Internet, much of which is unknown to users. Multiple theories on privacy attempt to explain this enigma, especially as users regularly face a tradeoff between disbursing personal information in return for personalization of products and services on the Internet.

These concepts also apply to mobile applications (mobile apps) on smartphone devices. The device's capabilities enable such activities as the Internet, e-mail, music and movie players, cameras, GPS navigation, and voice dictation in a centralized location for convenience and efficiency. Since a smartphone uses the Internet, evidence on online privacy can translate to mobile privacy. Mobile apps are the software that powers a smartphone. Individuals are fearful of relinquishing personal information to other parties based on concerns for data collection, data sharing, and data storage by creators of mobile apps.

Creators of mobile apps understand users' privacy concerns, and have instruments to respond to these concerns. Privacy policies exist to communicate companies' information-handling practices; and for the purposes of this paper, specifically in mobile apps. The essential elements of privacy policies of mobile apps are the language choices made by the companies that own the apps, and subsequently write the policies for the apps. Previous research identifies five common elements of online privacy policies including words or phrases on agents, claims, determinants, frequency, and relevant qualities. The context of the language matters in its effectiveness of moderating users' privacy concerns.

Mobile apps offer features in attempt to mitigate concerns in actionable ways by the creators. These features can be viewed as control mechanisms in that the services offer functions on behalf of users' privacy concerns to varying degrees. Currently, there are not enough sources of information on these control mechanisms, and the capacities in which these mechanisms answer to users of mobile apps.

This paper develops a foundation for the trifecta of users' privacy concerns; privacy policy language; and control mechanisms relevant to mobile apps. Specifically, social network apps that are increasingly popular and, arguably, the most notable source of users' concerns for privacy in the 21st century. The goal of this research is to investigate how certain social network apps address users' privacy concerns in the language of privacy policies, and to what extent do in-app control mechanisms meet these concerns, as well.

To begin, this body provides a background on online privacy, especially in regards to users' concerns in that environment; language of online privacy policies; and some current recognized control mechanisms. Identification of the selection process of the social network apps, Facebook, Instagram, Twitter, and Snapchat, follows the background information. The analysis focuses on the privacy policies and control mechanisms of each app on users' privacy concerns of: data collection, data sharing, and data storage; and the language of: agents, claims,

determinants, frequency, and relevant qualities. A discussion of the evaluation of the apps and the limitations of this paper comes after the analysis. Finally, conclusions are made on if social network apps duly respond to users' privacy concerns through privacy policies and control mechanisms.

Literature Review
Online Privacy in Mobile Apps

Definition of Privacy

A strict definition of privacy is non-existent because privacy issues depend on individual values and concerns (Westin, 1995; as cited in Viseu, Clement, & Aspinall, 2003, p. 3). There is the legal approach to privacy, according to Gellman (as cited in Viseu, Clement, & Aspinall, 2003, p. 3) privacy is fair information practices determined by self. Burgoon et al. discusses privacy in an active manner, "…as what, when, and how information about the self will be released to another person or organization," (as cited in Buchanan, Paine, Joinson, & Reips, 2007, p. 158). Similarly, to Burgoon et al. is DeCew's view of privacy as an, "acquisition or attempted acquisition of information that involves gaining access to an individual," (as cited in Buchanan, Paine, Joinson, & Reips, 2007, p. 158). Privacy can be an objective topic, but the underlying notion is of the individual relinquishing information about herself. This is an ambiguous and versatile introduction to privacy but can be clarified with review.

Privacy interests focus on the use of personal information. The United States Department of Labor defines personal information as, "any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect (United States Department of Labor). From the aforementioned definitions of privacy, privacy concerns arise from the perception that personal information is used unfairly (Culnan & Armstrong, 1999, p. 105). Corresponding with this note is Campbell's judgment that information privacy concerns are, "…an individual's subjective views of fairness within the context of information privacy," (as cited in Malhotra, Kim, & Agarwal, 2004, p. 337). Information privacy, or privacy of personal data, is, "the individual claim that data about themselves should not be automatically available to other individuals and organisations, and when it is, the individual must be able to exercise a substantial degree of control over that data and its use" (Clarke, 1999, p. 60). Based on these subjects, privacy concerns are the use of personal information data by businesses beyond individuals' awareness, and individuals' interpretations of fair-handling of that information.

Privacy in an Online Context

In an online context, Westin found attitudes about privacy translated in that 81% of surveyed Internet users considered privacy while online (as cited in Cranor, Reagle, & Ackerman, 1999). A separate survey presented a majority of respondents, with different values on privacy, all indicated high levels of concern for online privacy, specifically (Cranor, Reagle, & Ackerman, 1999). Other bodies of evidence support a majority of online users worried with online privacy maintenance in efforts to keep their personal information confidential (Sheehan, 2000, p. 21).

Several theories exist that attempt to explain privacy concerns on the Internet. Eisenhardt defines the agency theory as the relationship between the principal and the agent; whereas information about the agent is incomplete and the principal is unable to fully control the agent's behavior, which allows the agent to act in a self-serving way (as cited in Li, 2012, p. 472-473). On the Internet, a user (the principal) submitting personal information to a website (the agent) in exchange for goods and services exemplifies an agency relationship.

Asymmetry of information occurs because the business that owns the website has control over the user's information during and after the exchange. Donaldson and Dunfee detail the social contract theory which states the exchange of personal information from user to website is not only for an economic purpose, but a social purpose (as cited in Li, 2012, p. 472-473). This establishes a, "social contract," of mutually understood social norms for the two parties that reduces the risk of nonadherence by either party. The user submits personal information to the website under the assumption that the website will not misuse the personal information. If a user feels the website will not adhere to a social contract between the two parties, then the user may not exchange personal information with the website. The social contract theory also interprets the concept of fairness within the limits of users' control. The website fairly accepts the user's personal information when she learns of the website's intentions with the information. This gives the user control. The intentions of collectors of personal information will be evaluated in a separate section.

Privacy Paradox

Amidst online privacy concerns, a paradox exists between a consumer giving personal information to a website in return for personalization. Online personalization is the combination of technology and user information that fit a product or service from a business for a user, and the ease of accessibility the user has to the product or service (Chellappa & Sin, 2005, p. 184).

Other theories aid in explaining the tradeoff between privacy concerns and personalization. The uses and gratifications theory based on work from Klapper, Lin, McGuire, and Rubin considers two different categories of gratification users receive from a medium such as the Internet (as cited in Sutanto, Paime, Tan, & Phang, 2013, p. 1143-1146). Process gratification justifies that consumers use a medium for the experience; that of a user enjoying the technology (Sutanto, Paime, Tan, & Phang, 2013, p. 1144). Content gratification describes interest in the content it bears; that of a user enjoying the information (Sutanto, Paime, Tan, & Phang, 2013, p. 1144). Stafford and Stafford explain process gratification on the Internet resembles, "aimless surfing," (as cited in Sutanto, Paime, Tan, & Phang, 2013, p. 1144). From the uses and gratifications theory, the argument is that if users enjoy the process of using the technology, the technology will be used more regardless of content; such as aimless surfing (Sutanto, Paime, Tan, & Phang, 2013, p. 1144). Users incline towards online personalization with increased frequency of use of the Internet (the process), despite privacy concerns (the content).

In Petrino's, Stanton's, and Stam's research, the information boundary theory explains individuals form information areas around themselves with boundaries of readiness to disclose

information (as cited in Sutanto, Paime, Tan, & Phang, 2013, p. 1146). The consumer decides the actions that disrupt the personal information boundary (Sutanto, Paime, Tan, & Phang, 2013, p. 1146). In the instance of the privacy paradox, the user contemplates if sharing personal information within the boundary is worth the personalization from an application. The individual could perceive disseminating personal information as high risk because the action increases privacy concerns; such as a lack of control over the information or a vacancy of benefits (Sutanto, Paime, Tan, & Phang, 2013, p. 1146). In turn, a shortage of gratification.

The equation:

$$U(X) = \text{Benefit} - \text{Cost}$$

illustrates the consumer's utility function and the tradeoff between the exchange of information for personalization. The benefit is the amount of personalization received by the consumer and the cost is the consumer concern for online privacy (Awad & Krishnan, 2006, p. 18). The cost component in the equation is a function of consumer privacy concern, previous privacy invasion, consumer-rated importance of information transparency, and consumer-rated importance of privacy policies (Awad & Krishnan, 2006, p. 18). The benefit of receiving personalization from an application must be greater than the perceived cost by the consumer from those factors. A study found, in general, consumers are less willing to partake in online personalization if there is a greater concern for privacy (Awad & Krishnan, 2006, p. 19).

The study that measured consumer willingness to partake in online personalization against privacy concerns also explored the effect of information transparency. The result was consumer-rated value of information transparency increased with consumer-rated value on the existence of a privacy policy (Awad & Krishnan, 2006, p. 19). This implicates the significance of a privacy policy that discerns and communicates a firm's intentions with consumer information.

Trust in Online Privacy

The perception of trust between businesses and consumers in an online domain is worth noting. The online interactivity of businesses and consumers, with acknowledgement and maintenance of privacy concerns, allows for the establishment of relationships between the two parties. Trust is the confidence in reliability and integrity of a partner in an exchange (Morgan & Hunt, 1994, p. 23). Trust conceives meaningful relationships; such as users revealing personal information to businesses via websites (Wang & Emurian, 2004, p. 108). An attitude of trust towards an organization's website lessens online privacy concerns of consumers in disclosing personal information (Wang & Emurian, 2004, p. 106). Businesses can influence trust through site appearance; strong graphic, structure, content, and social-cue designs are trust-inducing features on a website (Wang & Emurian, 2004, p. 116).

If a consumer visually confirms trust via website, it is more likely the consumer will disclose personal information. A study found that a reputation prior to online interaction positively influences the trust relationship between businesses and consumers (Eastlick, Lotz, & Warrington, 2003, p. 883). If a consumer is aware of a brand before a website visit, she will more easily disclose personal information. Informed consent tells users the potential harm or

benefit an online interaction creates, and the opportunity to accept or decline participation in that interaction (Friedman, Kahn, Jr., & Howe, 2000, p. 38). Items such as privacy policies and trust agreements presents users with the opportunity to accept or decline online interaction with a business. The presence of these documents on a website can build trust and appease privacy concerns, which can give way to submission of personal information. However, no methods exist to ensure a trusting relationship between businesses and consumers, especially over the Internet; or that a user will contribute her personal information to an organization's website.

User Concerns for Online Privacy in Mobile Apps

The essence of mobile apps admits to access of personal information of users. Mobile apps necessitate user input. Users commonly store information describing preferences in contacts, messages, notes, locations, media, email, and more intrinsically on the device. This information, in conjunction with mobile apps, in a centralized location on a singular device make it easier to access personal information.

Online privacy concerns exist in relation to mobile apps since these programs require the Internet to function on mobile devices. A study specific to mobile apps explored the idea of privacy revelations, which are the, "automated descriptions of the spread of personal information based on measurement and analysis made by the operating system," (Wetherall, Choffnes, Greenstein, Han, Hornyack, Jung, Schechter, and Wang, 2011, p. 2). Privacy concerns of mobile apps stem from a lack of awareness on information-handling practices of the creators of mobile apps. The continued frequency of privacy aloofness in mobile apps further suggests users cannot perceive how companies use collected information. The fear of the unknown for users instantiates privacy concerns.

Online concerns for privacy in mobile apps range in subject matter. Smith et al. studied four dimensions of privacy concerns such as collection, unauthorized secondary use, improper access, and errors (as cited in Malhotra, Kim, & Agarwal, 2004, p. 338). Originally, these privacy concerns were studied offline, but the application of these concerns transcend environments. These concerns are noted in the following sections.

Data Collection

Collection in an online context is, "…the degree to which a person is concerned about the amount of individual-specific data possessed by others relative to the value of benefits received," (Malhotra, Kim, & Agarwal, 2004, p. 338). A user has a low degree of concern for collection when more benefits are received in exchange for submission of personal information; versus a high degree of concern about collection when less benefits are received in exchange for personal information.

Improper collection

The online privacy concern for collection encompasses improper collection. Improper collection means, "to collect a consumer's private information from the Internet without notice to, or acknowledgement from, the consumer," (Wang, Lee, & Wang, 1998, p. 65). In an online setting,

private information can include an email address, types of software, Internet history, etc. (Wang, Lee, & Wang, 1998, p. 65). Other inconspicuous methods of collection include automatic data transfer from web browsers in the form of cookies as outlined by Berman and Mulligan (as cited in Brown & Muchira, 2004, p. 66). A business may collect private information via a consumer's Internet history for self-serving needs, such as Web-based advertisements (Wang, Lee, & Wang, 1998, p. 65). A consumer realizes this action on behalf of the business and the levels of concern for online privacy increase.

Perceived intrusion is an example of improper collection of consumers' data. This means to invade user activities, such as the increasing issue of malware on mobile devices accessing browser history, usage patterns of mobile apps, phone numbers and keyboard strokes (Xu, Gupta, Rosson, Carroll, 2012, p. 4-5). This information collection through invasion with malware obviously goes against consumers' consent. Improper collection in some mobile apps also consists of messages, images, locations, and other mobile app login information. This data was found across eight different mobile dating apps (Farnden, Martini, & Choo, 2015, p. 4-9).

Data Sharing

Improper access

Online privacy concerns about improper access involve, "the infiltration of an Internet consumer's private computer without notice to or acknowledgement from the consumer," (Wang, Lee, & Wang, 1998, p. 65). Improper access can divulge personal information about a user (Wang, Lee, & Wang, 1998, p. 65). Malignant programs can attach to devices from the Internet and access credit card information clearly without consent from consumers (Wang, Lee, & Wang, 1998, p. 65). One form of improper access is unwanted solicitation; such as repeatedly contacting users that have not requested contact including messages such as junk email or pop-up windows (Brown & Muchira, 2004, p. 65). In the instance a user views and receives online messages outside of the initial visit to a site, the user experiences concern for her privacy.

Improper access occurs on mobile apps, as well. Tools such as permission analysis, static code analysis, network analysis, and dynamic flow analysis reveal that apps excessively access sensitive information (Lin, Amini, Hong, Sadeh, Lindqvist, & Zhang, 2012, p. 502). A characteristic of improper access that users are concerned about is perceived surveillance; or the judgement that mobile apps are carefully watching, and recording, users' decisions. Perceived surveillance of mobile apps provides for a high amount of information accessibility because mobile apps constantly monitor user actions (Xu, Gupta, Rosson, Carroll, 2012, p. 4-5).

Mobile apps access various types of personal information. A study investigated the comfort levels of participants in regards to mobile apps accessing the sensitive resources of network location, GPS location, device ID, and contact list (Lin, Amini, Hong, Sadeh, Lindqvist, & Zhang, 2012, p. 504-505). Participants were very uncomfortable with mobile apps accessing contact

lists, device IDs, and network locations. Furthermore, participants generally could not significantly discern the reason for mobile apps accessing that information.

Unauthorized secondary usage

Unauthorized secondary usage equates to lack of confidentiality and control for users (Brown & Muchira, 2004, p. 65). In Nowak's and Phelps' work, a user that submits personal information inadvertently allows the creators of the website to build a profile around the user pertaining to personal characteristics and lifestyle choices for use beyond the initial exchange of information (as cited in Brown & Muchira, 2004, p. 65). Improper analysis occurs when conclusions, such as preferences, are drawn from the collection of personal information from a user without consent (Wang, Lee, & Wang, 1998, p. 65). The user did not explicitly grant permission for secondary use of personal information. The privacy concern for unauthorized secondary usage can include usage outside of a singular website for an organization. Online privacy concerns about unauthorized secondary use of personal information consist of businesses selling, sharing, and publishing, personal information from users (Wang, Lee, & Wang, 1998, p. 65). Once a business obtains personal information from a user and creates a profile around the user, the business could transfer this information to other businesses without notice from the user (Wang, Lee, & Wang, 1998, p. 65).

Similar to general online privacy concerns, secondary use of information on mobile apps happens when creators use consumer information without consent. For example, a mobile app selling information to third parties that market the advertisements in the app to users' preferences based on decisions made in the app, and subsequently recorded as data (Xu, Gupta, Rosson, & Carroll, 2012, p. 5). Users become aware of instances of secondary usage when advertisements relevant to previous choices made in the app display as banner advertisements or pop-up windows. The notification of these advertisements by the user institutes the concern for unauthorized secondary usage.

Data Storage

Improper storage

Improper storage is, "to keep private information in a non-secure manner resulting in a lack of trustworthiness of the stored information, or lack of authentication control for information access," (Wang, Lee, & Wang, 1998, p. 66). Improper storage prevents data integrity and facilitates errors in accuracy of personal information. Errors can happen because of improper storage of the vast amount of personal information collected from users (Brown & Muchira, 2004, p. 66).

Due to the expanse of services mobile apps offer users such as social networking, banking, shopping, email, and calendar and address book functions; much personal information is stored including login credentials, credit card details, and purchase orders (Jain and Shanbhag, 2012, p. 29). Mobile apps can disclose this information if data is left unprotected by the user or the app because best practices for security are not followed.

Due to consumers' want for mobile applications to meet needs, and businesses' desires to make profits with mobile applications, an agreement establishes the information exchange between the two parties. A mutual understanding is reached between consumers and businesses with privacy policies that address these concerns prior to information exchange between the two parties.

Privacy Policies in Mobile Apps

Online Privacy Policies

Businesses create privacy policies that outline information-handling practices to meet privacy concerns of users. Privacy policies help inform consumers, so that consumers can decide to continue interaction with the business or not (Jenson & Potts, 2004, p. 471). A user may decide to discontinue communication with a business, through a website or mobile app, upon learning of the conduct of personal information based on individual determination of fair use of that information. Privacy policies must be relatable, accessible, and readable to adequately address user concerns about online privacy.

In general, privacy policies address the information-handling practices of data collection, data retention, data sharing, data destruction, and data protection (Pollach, 2007, p. 105). Pollach's study used factual coding to analyze 50 companies' online privacy policies, and found medial percentages relating to coverage of the above practices (Pollach, 2007, p. 105). Of the policies, 27.6 percent, 75.0 percent, and 37.5 percent identified methods for data collection, data storage, and data sharing, respectively, in the text (Pollach, 2007, p. 105). These are insignificant percentages, but it is worth noting that research shows data-handling practices are found in privacy policies. The services provided by the Internet and mobile apps are identical; the difference being mobile apps accommodate for more convenience. The assumption will be made that privacy policies of mobile apps layout the same content as online privacy policies. However, the language of privacy policies will be applied to mobile apps.

Language of Online Privacy Policies in Mobile Apps

There are different modes to address privacy concerns of users of mobile apps with language. Privacy policies systematically use words or phrases that negate and passively focus on topics (Pollach, 2007, p. 106). Pollach's study characterizes five purposes for the language in privacy policies. These five ideas will serve as the foundation for the analysis of the language of the privacy policies of the mobile apps involved in this discussion. These subjects and certain words or phrases, and the connection to user privacy concerns, are noted in the following sections.

Agents

Agents are often removed from words or phrases in privacy policies. Nouns are left out of words or phrases such as, "the sharing of, is shared, and you receive," (Pollach, 2007, p. 106). Omission of assignment of words or phrases with explicit nouns depreciates the responsibilities of businesses. This ambiguity leaves uncertainty for who is liable for leakages of users' personal

information. Businesses can be exempt, while maintaining authentic privacy policies, with words or phrases that remove agents from the language.

Claims

Claims in the language of privacy policies refer to commitments from the business. These words or phrases, again, put control in businesses' hands about the handling of users' personal information. Also, businesses' can include these words in regards to changing policies however deemed necessary. Words or phrases that pertain to claims from businesses are, "may, might, perhaps, in/ at our discretion, except as, on a limited basis, we reserve the right to, including but not limited to," (Pollach, 2007, p. 106). It is at the discretion of the business whose policy contains these words or phrases if these practices are followed.

Determinants

Privacy policies use words or phrases that give users the authorization to deny or accept companies' information-handling practices. This happens when users accept the terms and conditions of the privacy policy; and usually only occurs once when users download, open, and create an account on a mobile app. These words or phrases can allow companies to, again, change privacy policies, but without informing the user. Words or phrases that enable those actions are, "if you authorize us, only when authorized, not without your consent/ permission/ knowledge, when we have your permission, not… unless you give us the permission to do so," (Pollach, 2007, p. 106).

Frequency

The frequency of language in privacy policies relates to the use of words or phrases such as, "occasionally, from time to time, sometimes, and at times" (Pollach, 2007, p. 106). The vagueness of these words or phrases signify the regularity of companies' information-handling practices. It is apparent from this language that it is at companies' discretions, not consumers' discretions, how personal information is collected, shared, and stored. However, the user consents to these occurrences, as exemplified by statements like, "[Company name] may change this statement from time to time" (Jenson & Potts, 2004, p. 476).

Relevant qualities

The language of privacy policies uses words or phrases that assert qualities of the businesses. Words or phrases that illustrate these qualities are, "trustworthy, reputable, carefully selected, and of interest/ value to you," (Pollach, 2007, p. 106). This especially pertains to data sharing with companies outside of the original contact with the business. Specifically, contact with the mobile app.

Control Mechanisms of Mobile Apps

Definition of Control Mechanisms

Control mechanisms answer users' online privacy concerns and demonstrate the language of privacy policies in tangible ways. These control mechanisms are the various features mobile

apps offer to moderate users' privacy. The features are actionable means for businesses to address users' privacy concerns, and implement privacy policy language; which creates a connection between the two aforementioned conditions.

Recommended Control Mechanisms

Several control mechanisms exist as recommendations from other bodies of research that found issue with privacy on smartphones. One suggested control mechanism would be an additional permission specification for the Android system called TISSA to protect phone identity, location, contacts, and call log information from third-party apps downloaded by the user (Zhou, Zhang, Jiang, & Freeh, 2011, p. 96-97). A privacy setting content provider and privacy setting manager would actively monitor third-party apps for violations of the user's privacy settings across the device. In testing, TISSA effectively prevented the leakage of contacts and call log information once users selected the corresponding privacy setting. However, this assumes proactive intervention from the user; versus proactive, automatic intervention from the permission upon recognition of a leakage. Most research recommends the use of another system term to protect users' privacy concerns on the Android system.

A second recommendation for a control mechanism is a market-aware privacy protection framework that responds with a feedback loop based on advertisements to adjust users' privacy protection (Leontiadis, Efstratiou, Picone, & Mascolo, 2012, p. 1). This would be a third-party app that users would download, as well. The argument stands for the purpose of users downloading a supplementary mobile app from a third-party when users' privacy concerns originate in third-party mobile apps.

A third suggested control mechanism incorporates privacy policy language with a programming model that ensures the system adheres to the privacy policy by putting sensitive values (users' privacy concerns) into contexts that control how the values are disclosed (Yang, Yessenov, & Solar-Lezama, 2012, p. 85). These constraints are written into the code of third-party mobile apps. This mechanism was effective in its testing, but requires hard-coding of all privacy constraints. This intention is laborious as creators cannot practically address all individual privacy concerns, but more so general privacy concerns, before launching an app.

The preceding research does not deliberate current control mechanisms within mobile apps that allow users' options for privacy. Another discretion from the above conversation is that the recommended mechanisms were only for Android operating systems, not iOS; with the exception of the control mechanism that recommends writing language constraints into the code of all third-party mobile apps. Also, language of privacy policies of mobile apps in terms of coverage of current users' privacy concerns is not examined in the reviewed studies. There may be other investigations of control mechanisms, but these examples stand to merely proclaim the existence of control mechanisms for users' privacy concerns.

Control mechanisms can adequately lessen users' privacy concerns, yet these cases argue much effort must be put into developing new systems without reasoning why control

mechanisms within mobile apps do not already do so. A separate system is redundant if mobile apps inherently contain effective control mechanisms for users' privacy concerns. Moreover, users can take individual precautions to protect privacy beyond options offered within the app as a control mechanism to meet privacy concerns.

The purpose of this research is to deliberate the connection between users' privacy concerns in mobile apps to the language of the privacy policies and the control mechanisms offered as in-app features to assuage these concerns. The language of the policies is given attention for contextual reasons for users. The control mechanisms are meaningful behaviors of the creators of mobile apps. The methodologies section explains the selection process of the mobile apps and criteria for measuring the coverage of control mechanisms in congruence with users' privacy concerns and language of privacy policies.

Methodologies

Users' privacy concerns can hinder the relationship between users and creators of mobile apps. It is important that privacy policies, the main communication tool between businesses and consumers of mobile apps, appease these concerns in meaningful and succinct ways. The language of privacy policies aims to satisfy users' privacy concerns, but can be vague intentionally by the company and leave consumers unsure about use of the app. Control mechanisms are applications of the outline privacy policies give on the handling of users' privacy concerns through in-app features available for modification by users.

Generally, users' privacy concerns are addressed in privacy policies by topic, including data collection, data sharing, and data storage. Whereas certain statements highlight the frequency, relevant qualities, claims, determinants, and agents throughout the language of privacy policies in reference to companies' data collection, sharing, and storage activities.

This study examines choice words or phrases in terms of frequency, relevant qualities, claims, determinants, and agents in the privacy policies of mobile apps **(A)**; the in-app features that provide control to creators and users **(B)**; and how the language and in-app features address privacy concerns with functionalities that favor more control for either creators or users **(C)**. The privacy concerns a part of the evaluation of the language themes and control mechanisms of the mobile apps are data collection, data sharing, and data storage; as these concerns relates to improper collection, improper access, unauthorized secondary usage, and improper storage. Figure 1 illustrates the relationship this research anticipates to study:

(A) → (C) → (B)

Figure 1. Relationship between language themes and control mechanisms on user privacy concerns

Four mobile apps and privacy policies serve as evaluation for the argument; Facebook, Instagram, Twitter, and Snapchat. These mobile apps are not meant to be representative of all

mobile apps and privacy policies that discuss users' privacy concerns relevant to control mechanisms. The apps were chosen for this study because of their successes, measured by number of users and rankings in the App Store. Facebook has over 1 billion active users, and ranks number six on the Free section of the App Store's Top Charts. Instagram users total over 600 million, and is number four on the App Store's Free Top Charts. Twitter has over 300 million active users, but ranks the lowest on the App Store's Top Charts in the Free section at number twenty-five. Snapchat is the highest ranked free mobile app of the four on the App Store at number two on the Top Charts; it has over 300 million users, as well. Another commonality is that these four apps are free to download to users. These numbers are for the week of April 10, 2017.

In terms of the documents used to discern the apps' approaches to the circumstances, three out of four apps' privacy policies are explicitly titled, "Privacy Policy." However, Facebook's policy is titled, "Data Policy," and contains the fundamental information that pertains to privacy concerns. Other documents available from the apps were not viewed for this analysis. These policies were accessed for the week of April 10, 2017.

Analysis of Policies and Control Mechanisms

Facebook

Facebook's Data Policy (last revised on September 29, 2016) outlines the company's actions of data collection, data sharing, and data storage. Facebook collects data based on all information used within their Services. This personal information can include contact information (from an address book on a device); location; age; language; credit and debit card information; operating system, hardware, settings, file names, and mobile operator of a device; information from third-party websites that use Facebook's Services; and information from Facebook's companies and partners. Facebook uses this information to personalize content, such as suggestions within its services, provide shortcuts, and enhance features.

The app shares data between users that communicate with each other through its Services; apps, websites, and third-party integrations that use its Services; Facebook's family of companies; new ownership of Facebook; and third-party partners and customers such as advertising, measurement, and analytics services. Facebook stores data for as long as necessary to serve its users. In the instance of a change to Facebook's Data Policy, Facebook notifies users to allow them to review and comment on the altered policy prior to continuing use of the social network.

Data Policy Language of Facebook

Specific words or phrases from the Data Policy exhibit the themes of agents, claims, and frequency. Excerpts from the Data Policy demonstrate each theme below:

"**We** share information we have about you within the **family of companies** that are part of Facebook."

“Here are the types of **third parties** we can share information with about you: **advertising, measurement and analytics services and vendors, service providers and other partners.**”

Analysis: Both of these statements remove agents in favor of Facebook in terms of data sharing. The policy does not specifically use the name of the company when discussing data-handling practices. The phrases, “family of companies,” and, “third parties,” leaves the company’s partners unnamed. This ambiguity can increase users’ data sharing concerns because users cannot identify exactly what entities, besides Facebook, are accessing and using information from their accounts. If a user is not knowledgeable on members of Facebook’s family of companies, and a discrepancy occurs for the user with improper access or unauthorized secondary usage of information from the Facebook account; the user will not know how to correct those actions based on this data policy. The ambiguity favors Facebook in that it does not have to take responsibility for those discrepancies.

“**We’ll notify you before we make changes to this policy** and give you the opportunity to review and comment on the revised policy **before continuing to use our Services**.”

Analysis: The claim from Facebook is that it will notify users before changing the data policy; which is likely to affect all of the ways Facebook handles data, thus, all privacy concerns. The claim is of users having control to preapprove changes to the policy before continuing use of the app. Frequency of changes are not certain, but determined by the number of times users receive notice prior to policy changes. The user cannot expect changes, and the nature of this statement implies that changes are at the discretion of Facebook. Furthermore, there are no words that guarantee users’ reviews or comments on policy changes prior to implementation will result in amendment.

“We store data for **as long as it is necessary** to provide products and services to you and others, including those described above. Information associated with your account **will be kept until your account is deleted, unless we no longer need the data to provide products and services**.”

Analysis: In terms of data storage, the language uses frequency to imply to users that unless deletion happens, personal information can exist forever on Facebook. The longer the data storage, the more opportunities for improper storage on behalf of the company. The length of time for storage is at the discretion of Facebook, and not of users. Another example of control favoring the company over user concern. Also, once deletion occurs, information that was not posted directly by the user’s individual account remains on the app. This is in the same section of the policy in sentences following those above.

Control Mechanisms of Facebook

Facebook’s in-app features that meet users’ privacy concerns:

Activity Log Tool
Functions: Contains posts and actions from the original to the present use of the app. Can add or hide activity on Timeline; view if the information is private or public; and undo action that put activity in the Activity Log Tool.

Analysis: The Activity Log Tool offers users control over the actions of an account in terms of information sharing and storage. A user can choose to display certain content on the profile; this choice of what content is, or is not, a part of the profile helps to prevent improper access by other parties because of the user instructs Facebook what information can be accessed by the profile. Similarly, the choice to associate or delete information from the Activity Log Tool ensures the correct information stored with the account.

Advertising Preferences
Functions: Displays interests from pages liked on Facebook; previous interactions with advertisers; ad settings; and block ad topics.

Analysis: Advertising Preferences offers users control over data collection and data sharing with advertisers tailoring advertisements relevant to users' interests. The user controls information associated with the account for advertisements, and the information shared with advertisers beyond its original intention. Both of these choices on part of the user help to control improper collection and unauthorized secondary usage. In addition, advertisers control comes from the benefits of users' potential use of the products/ services advertised because of user election to see advertisements in coordination with their activities. Control is neutral.

Deactivation/ Deletion
Functions: Hides account information temporarily (user's profile and search result not visible to others); and/ or erases all information for the specific user's account (cannot reactivate or retrieve the profile).

Analysis: The options to deactivate and/ or delete an account offers users control over data storage with the account. Users can choose to hide account information temporarily from other users for an amount of time specified by the owners of the accounts. Users can delete the entire account, and remove all information stored with the account. The deactivation and/ or deletion of the account halts Facebook from collecting new data from the account, as well. Thus, stopping improper collection. Control for the user over the collection and storage of the account, and, subsequently, all information in the account, stems from the choice for removal.

Privacy Settings and Tools
Functions: Controls who can see future posts; tagged posts; audience of previous posts; who can send friend requests; and who can search based on email, phone, or search engines outside of Facebook.

Analysis: Privacy Settings and Tools allows users control over what she can deem private information. Ultimately, users can choose the other users that view information, and the type of information, from the account. The user's choice of other members that have access to posts, requests, etc. benefits proper access and inhibits improper access because the user will avert other users she does not want a connection.

Timeline and Tagging Settings

Functions: Controls who can change and view items on an account; who can post on Timeline (friends or other users); reviews tagged posts before appearing on Timeline; who can see Timeline; who can see tagged posts on Timeline; who can see others' posts on Timeline; and who can see tag suggestions when Facebook recognizes uploaded photos that look like the user.

Analysis: Timeline and Tagging Settings gives users greater control for those that can view, post, and tag to the account. Improper access and unauthorized secondary usage are prohibited because the user decides the other users' permissions to post (photos and shares) in association with the profile. Storage of these permissions for approved contacts is kept with the rest of the account information. Prevention of improper storage, improper access, and unauthorized secondary usage occurs because Facebook does not decide other users' permissions.

Social Reporting

Functions: Controls posts based on user preference that do not violate Facebook terms. The user can send a message to the owner of the post requesting removal.

Analysis: The Social Reporting feature of Facebook allows users control over potential removal of posts associated with the account. These posts are not automatically removed from Facebook because the posts do not violate Facebook terms of use, but the user may still find the posts offense or as violations of privacy. A user can choose to message the owner of the non-agreeable post for removal. If the post is removed, Facebook can maintain those interactions (the post, transmittal between users, etc.) to better understand the types of items that the user does not want associated with the account in the future, ensuring proper information collection. The removal of the post will also prevent unauthorized secondary usage because the user prevents other users from posting outside of the user's original concession with the post.

Instagram

Instagram's Privacy Policy (last revised on January 13, 2013) and a company of Facebook since 2012) pertains to its practices on data collection, data sharing, and data storage. Instagram collects data on information provided directly by the user; through searching for other users on Instagram; analytics information; cookies and similar technologies; log file information; device identifiers; and metadata. This collected data is used for logging-in; preventing redundancy of entering information; personalizing content; improving Services; monitoring

metrics; fixing technology problems; and automatically updating the app. Instagram shares this information with businesses that are legally a part of the same group of companies as Instagram; third-party organizations (service providers) that help provide the Service to users; third-party advertisers; and new ownership of Instagram. Users' information is stored until termination of an account, and can retain that information for some amount of time after account deletion.

Privacy Policy Language of Instagram

Specific words or phrases from the Privacy Policy exhibit the themes of agents, determinants, frequency, and relevant qualities. Below are examples of each theme from the Privacy Policy:

"But these **Affiliates will honor the choices you make** about who can see your photos."

Analysis: The themes of agents and determinants is shown by the bolded phrase above for the concern of data sharing. Instagram removes agents by using the word, "Affiliates," instead of naming its third-party partners. Agents are further removed throughout the policy with words like, "we," "you," and "service providers," to de-emphasize the authority and responsibility of actions from Instagram in relation to data sharing, such as with Facebook. This, again, allows the company more control with instances of users' privacy concerns. Although unnamed, the policy shows determinants because Instagram's third-party affiliates will be aware of users chosen to see the content of an account, and share content based on those users approved to see it. This gives the user discretion of sharing content with other users to view the account, but because the affiliates are vague to the user and at the discretion of Instagram, this is a neutral phrase in addressing the concern of data sharing.

"…may retain information (including your profile information) and User Content **for a commercially reasonable time** for backup, archival, and/or audit purposes."

"Instagram may modify or update this Privacy Policy **from time to time**, so please review it periodically."

Analysis: These lofty phrases are in reference to the frequency of data collection, data sharing, and data storage. The first phrase answers the concern for data storage as it discusses the length of time that Instagram keeps account information. A, "commercially reasonable time," could mean any amount of time, and it is up to the company to decide what length of time is appropriate for storage. This statement does not allow negotiation from the user, and relinquishes control to Instagram by using its services. The second phrase answers all privacy concerns because it acknowledges changes made to the privacy policy; which, again, are likely to affect all information-handling practices. Changes to the policy are at the discretion of Instagram, and dismisses responsibility from the company in updating users to changes to the policy. Users can unknowingly agree to different data-handling practices due to changes of the Privacy Policy. The user may not actually be in agreeance with these changes put forth after

creation of an account (and original acceptance of the policy); but by continuance of use of the app accepts these changes without notification from Instagram.

“This information would allow third-party ad networks to, among other things, deliver targeted advertisements that they believe **will be of most interest to you**.”

Analysis: The policy language uses relevant qualities to describe Instagram’s approach to advertisements on accounts through sharing data with third-party ad networks. The statement enhances user control because it implies that advertisers will display information compatible with interests. If advertisements pertain to content users elect to view; then the advertisements can further influence users, and the services in the advertisements have greater potential to reach consumers that have actual enthusiasm for those services. Users have control over the types of advertisements on the app, and Instagram’s third-party ad networks have control in that advertisements are shown on the app. A neutral approach to data sharing for both the creator and user.

Control Mechanisms of Instagram
Instagram’s in-app features that meet users’ privacy concerns:

Blocked Users
Functions: Control other users that cannot view profile.

Analysis: The Blocked Users function lets a user choose who can view the content. A user can select certain users to view (or not view) the profile if information on the account must remain hidden according to the user’s demands. Once blocked, users cannot access the profile, thus, preventing improper access.

Comments
Functions: Control comments left by other users by hiding inappropriate comments with keywords or phrases that are often reported as offensive; and/ or indicate keywords or phrases not to be displayed in comments.

Analysis: A user can choose to delete comments left on user content, and control words from appearing in any comment shared on the account. For example, a user can indicate the word, “ugly,” from ever being left in a comment on a photo or video because it offends the user; then other users cannot see the comment with the word, “ugly,” in it, and associate that word with the account.

Edit Profile Option
Functions: Displays name, username, website link, biography, and photo; and stores email, phone number, and gender.

Analysis: A user creates unique information to enhance the identification of the account. A user ensures correct information collection and storage by Instagram for its services by the user entering the unique information in the Edit Profile Option.

Linked Accounts

Functions: Control settings of other social networks integrated with Instagram in one location.

Analysis: The Linked Accounts tool allows users to connect social media accounts for cross-posting functionality. For example, a user can allow Instagram to access information from that user's Facebook or Twitter accounts. This connection can assure the appropriate information collection across accounts. This is an option, not a requirement, of a user, but choosing to connect accounts allows Instagram access to information across both accounts. However, Instagram is a part of Facebook's family of companies, and based on both companies' privacy policies, user information is already shared across networks. This access could possibly be for ulterior purposes. This tool attempts to give the user control, but has underlying control by Instagram because it is owned by Facebook.

Private Account

Functions: Controls other users approved to view a user's photos and videos on Instagram; but does not affect existing followers.

Analysis: This feature permits users to hide content from the entire population of Instagram by only allowing certain users to view the account via consent from the owner of the content. This enables the user to control sharing the data of the profile; since a user can choose other users access to the account, this feature helps to control improper access by unapproved entities.

Story Settings

Functions: Hides story and live videos from specific users; allows message replies from followers; and saves shared photos to the device.

Analysis: Story Settings authorizes the user to prevent certain other users from viewing the user's content of stories and live videos, replying to those stories and live videos; and saving those stories and live videos to the device. The user's prevention or permission of others to view this content is what places control in the user's hands, and hinders improper access of the account. Also, the user's ability to save the content to the device prevents improper storage because the user chooses to save or not to save.

Two-Factor Authentication

Functions: Requires a security code to enter when logging-in to verify identity of the user.

Analysis: Two-Factor Authentication lets a user implement a secondary log-in verification code to avoid improper access to the account. The user does not have to implement a secondary log-in verification with the account, but has the choice to if the user wants to take extra measures for security.

Twitter

Twitter's privacy policy (last revised on September 30, 2016) has sections on information collection and use, and information sharing and disclosure. There is not a specific section on storage practices, but a few statements throughout the policy indicate how Twitter stores information. Twitter's policy blatantly states that a Tweet becomes public by default when sent. The platform further collects the following information from users: name; username; password; date of birth; email address; phone number; credit and debit card information; address book from device; account information from other services connected to Twitter; location; photos; metadata such as date and time of Tweet, application used to Tweet; language; followers; direct messages; wireless networks; IP addresses; links; cookies; operating system of device; and mobile carrier.

Twitter uses this information for log-in; personalization; commerce; advertisement; statistic; and improvement purposes. Twitter uses this information for log-in; personalization; commerce; advertisement; statistic; and improvement purposes. Users' information is shared based on user consent; service providers; law; business transfers and affiliates; and non-personal information. In terms of storage, Twitter deletes Log Data after 18 months, and deletes information from cross-posting between Twitter and other accounts after disconnecting the accounts. The Twitter Privacy Policy does not state the exact amount of time the company stores other information; assumption is made until deletion of the account.

Privacy Policy Language of Twitter

Specific words or phrases from the Twitter Privacy Policy exhibit the themes of agents, claims, determinants, and frequency. The Twitter Privacy Policy shows each theme in different contexts below:

"When **you** share information or content like photos, videos, and links via the **Services**, **you should think carefully** about what you are making public."

Analysis: The policy language theme of agents is present for Twitter's information-handling practices; specifically, for data sharing on part of the user. The word, "you," refers to the user reading the policy. It is impersonal and allows Twitter to speak to whoever reads the policy. Also, "Services," is a broad term that covers current and future offerings of the company. Individually, these terms do not hold weight in the mind of the user. Beyond that, the entire statement puts all responsibility on the user. The statement gives Twitter less liability for instances of improper access and unauthorized secondary usage. Once content is in a Tweet, it is public information; and Twitter can, essentially, handle that information without obligation despite this policy detailing other information-handling practices.

“If we make a change to this policy that, **in our sole discretion**, is material, we will notify you via an @Twitter update or email to the email address associated with your account.”

Analysis: Claims are used with the topic of changes to the policy, and, by association, the concerns of data collection, data sharing, and data storage. Obviously, “in our sole discretion,” puts all control in Twitter when deciding on the handling, and/ or how to change the handling of users’ information. Also, Twitter determines if these changes are significant enough for users to receive notice. Changes that Twitter deems immaterial may be significant to some users, but this line states that it is up to Twitter to tell users their own concerns.

“We may share or disclose your information **at your direction**, such as when you authorize a third-party web client or application to access your account or when you direct us to share your feedback with a business.”

Analysis: On the contrary, a determinant is in the bolded phrase above that allows users the clear authorization to deny or accept Twitter’s actions relevant to data sharing. Twitter will share information with third-parties, but at the discretion of the user indicated by the user’s actions pertinent to the app. However, with the phrase, “in our sole discretion,” existing in the same policy, the phrase, “at your direction,” can implicate a false sense of control to users.

“Twitter **broadly and instantly** disseminates your public information to a wide range of users…”

“We may revise this Privacy Policy from **time to time**.”

Analysis: Frequency in Twitter’s privacy policy appears in a couple of phrases attributable to all data-handling practices. “Broadly and instantly,” can imply a total loss of control for the user due to the speed and disbursement of information. A user may accidentally share sensitive information (that Twitter will not protect) dependent upon the account’s security settings, whether known or not to the user. Similar to other policies, the frequency of changes to the policy that happen, “from time to time,” gives Twitter, not the user, discretion for policy changes it sees fit.

Control Mechanisms of Twitter

Twitter’s in-app features that meet users’ privacy concerns:

Account Settings

Functions: Adds, edits, or removes username, phone number, email address, and secondary security log-in verification to the account.

Analysis: Twitter appeases all users’ privacy concerns with the Account Settings feature. A user can confirm correct collection and storage by entering unique identification information with the account in a username, phone number, and email address. Also, the secondary security log-in verification option is an extra precaution the user can take to inhibit improper access. If another

entity beside the user attempts to access the account, the secondary log-in verification is another step the entity will have to bypass.

Privacy and Safety Settings
Functions: Protects Tweets so only current followers and approved users can view; tailors advertisements based on ad partners; allows other users to search the account by email, address, or phone number; searches other users based on address book from device; and blocks and mutes other users accounts.

Analysis: Privacy and Safety Settings give the user more control with options to conserve the information in association with a user's Twitter account. The concern for data collection is mitigated because users can choose to tailor advertisements, certifying proper data collection, to display relevant advertisements with the user's interests. The user can choose to hide tweets from other entities, halting improper access and unauthorized usage of the user's Tweets because other entities do not have permission to view the content.

Timeline Settings
Functions: Displays Tweets at top of timeline that are likely to be more popular according to the user's preferences.

Analysis: Twitter takes the initiative to showcase suitable content according to data collection from the account. The user could benefit from this feature with proper information collection, but if improper collection comes from the account the user could feel that Twitter is presumptuous with irrelevant Tweets towards the user's interests at the top of the timeline. If this function is enabled, the user does not have a choice of what Tweets are at the top of the timeline. Those Tweets will be based on Twitter's algorithm; which makes this a neutral control mechanism for concerns about data collection.

Snapchat
Snapchat's privacy policy (last revised on April 12, 2017) has distinct pieces in its privacy policy on data collection, data sharing, and data storage. Snapchat collects information about users such as names; username; password; email address; phone number; date of birth; location; address book from device; photos; debit and credit card information; in-app photo and text messages; friends list; communications between user and Snapchat support; in-app photo filters; search queries; date and time of communications; interactions with messages; metadata; device information; operating system; IP address; cookies; and information from third-parties about the user.

Snapchat uses this information for a multitude of reasons. These reasons are to develop, operate, improve, deliver, maintain, and protect Snapchat's products and services; send communications; monitor and analyze trends and usage; personalize services; contextualize experiences; improve advertising; enhance security of products and services; and to, overall, enhance services and experiences. Snapchat shares this information with other users; the

services in the app; business partners; affiliates; third-parties; and the general public if allowed by the type of information. Photo and video messages are automatically deleted from the servers after the servers detect that those messages were opened or expired; but different servers may have different deletion instructions dependent on the storage of the messages based on content. An account must be deleted, or deactivated for 30 days and then deleted, for all servers to remove account information.

Privacy Policy Language of Snapchat

Specific words or phrases from the Privacy Policy exhibit the themes of claims, frequency, and relevant qualities. Portions of the Privacy Policy to present for each theme are below:

"Keep in mind that, while our systems are designed to carry out our deletion practices automatically, **we cannot promise** that deletion will occur within a specific time frame."

Analysis: The policy uses claims to speak on the privacy concerns of data sharing and data storage. Snapchat cannot guarantee the deletion of user content within a distinct time frame; meaning that it is stored for longer than a period of 24 hours, which is the assumption of users. If not deleted within 24 hours, user content will be stored longer than assumed, which could lead to instances of improper storage. The user cannot be sure the content, if stored longer, will not be accessed or used beyond its original intention by others. This denial from Snapchat can heighten user concerns for data sharing and data storage because it contradicts users' assumption of data-handling practices by the company.

"We may change this Privacy Policy **from time to time**. But when we do, we'll let you know one way or another. **Sometimes**, we'll let you know by revising the date at the top of the Privacy Policy that's available on our website and mobile application. **Other times**, we may provide you with additional notice (such as adding a statement to our websites' home pages or providing you with an in-app notification)."

"Outside of Snaps, the rest of our services may use content **for longer periods of time**, which means those services may follow different deletion protocols."

"Or if you submit content to one of our inherently public features, such as Live, Local or any other crowd-sourced service, **we may retain the content as long as necessary** to offer and improve the services."

Analysis: A number of phrases express frequency surrounding all user privacy concerns with data collection, data sharing, and data storage. "From time to time," "Sometimes," and "Other times," display Snapchat's possible actions to modify the privacy policy. The phrases give Snapchat discretion to make changes, and subsequently notify users of those changes. None of those phrases give a specific time for users to anticipate changes, or a guarantee to users to receive notice of changes that are likely to affect all data-handling practices. On data sharing and data storage, Snapchat states that it can use content, "for longer periods of time." This

phrase is obscure to users because it removes a specific time frame, again, and opposes the assumption of Snapchat's services. Snaps and Chats sent to other users, but used beyond original intention by other entities, especially after a 24-hour period, justifies the concerns for improper access; unauthorized secondary usage; and improper storage. Data storage, and furthermore improper storage, concerns are emphasized with the phrase, "we may retain content as long as necessary," because, again, a distinct time frame is not in the policy when the assumption is a 24-hour period. These numerous examples demonstrate the contradiction of the existence of data-handling practices by Snapchat because these practices are without guarantee.

"What do we do with the information we collect? The short answer is: provide you with an **amazing** set of products and services that we **improve relentlessly**."

Analysis: Snapchat attempts to illustrate relevant qualities for itself with positive words and phrases that highlight its commitment to data collection. These words and phrases attempt to be pro-user in explaining the reasons for collection information from user content. However, this is one statement in the policy; whereas most of the policy uses language that defects from the user and orients more towards protecting company actions. One statement may not be enough to assuage users' privacy concerns.

Control Mechanisms of Snapchat
Snapchat's in-app features that meet users' privacy concerns:

Ad Preferences
Functions: Controls in-app advertisements based on information collected outside of app from third-party services.

Analysis: This control mechanism gives users control over data sharing with advertisers to customize in-app advertisements based on data collection. Once the user elects to have ad preferences active on the account, Snapchat's ad partners can collect accurate information representative of the user's interests for advertisements. This choice on part of the user instantaneously allows ad partners to use the Snaps and Chats from the account to tailor advertisements to the interest of the user based on the content from these interactions. This becomes an authorized secondary usage of the user's content in the app.

Blocked
Functions: Controls other users that can view the user's Story and send Snaps or Chats.

Analysis: The Blocked function lets a user choose who can and cannot view the user's content. This helps a user control improper access by other parties when sharing the data of the account because, once blocked, other parties cannot access the user's content.

Contact Me

Functions: Controls if all users or users on the friends list can contact the user directly.

Analysis: The user can choose the other users, all Snapchatters or only those on the user's friends list, that can contact the user through the app. This shares permissions and assigns access to others, which helps to heed the concern of improper access. This favors the user's control over Snapchat's control.

Deactivation/ Deletion
Functions: Hides account information temporarily (user's profile not visible to others); and/ or erases all information for the specific user's account (cannot reactivate or retrieve the profile).

Analysis: The options to deactivate and/ or delete an account offers users control over data storage with the account. Users can choose to hide account information temporarily from other users for an amount of time specified by the owners of the accounts. Users can delete the entire account, and remove all information stored with the account. The deactivation and/ or deletion of the account halts Snapchat from collecting new data from the account, as well. Thus, stopping improper collection. Control for the user over the collection and storage of the account, and, subsequently, all information in the account, stems from the choice for removal.

Login Verification
Functions: Uses a verification code, in conjunction with the username and password, to log-in on new devices.

Analysis: Login Verification lets a user implement a secondary log-in verification code, in conjunction with the username and password for the account, to avoid improper access to the account. The user does not have to use the Login Verification feature with the account, but has the choice to if the user wants to take extra precautions.

View My Story
Functions: Lets the user choose who can view the Story (everyone, friends, or custom).

Analysis: View My Story gives the user control over other users' abilities to view the Story feature on the user's Snapchat account. The user receives control when she grants permission to other users to view the Story. This permission is what counters improper access because the user permits proper access by the appropriate parties. In granting permission to other users, the user authorizes those to use the content in the Story beyond its original intention because of the nature of Snapchat; in posting a Snap or Chat, it becomes public information.

The language and control mechanism findings from all of the mobile apps are summarized in Table 2 and Table 3, respectively, and discussed in the following section:

	Statement(s)	Language theme(s)	User privacy concern(s)	Control
Facebook	“We share information we have about you within the family of companies that are part of Facebook.” “Here are the types of third parties we can share information with about you: advertising, measurement and analytics services and vendors, service providers and other partners.”	Agents	Data sharing · Improper access · Unauthorized secondary usage	Pro-app
	“We’ll notify you before we make changes to this policy and give you the opportunity to review and comment on the revised policy before continuing to use our Services.”	Claims	Data collection, data sharing, and data storage	Pro-app
	“We store data for as long as it is necessary to provide products and services to you and others, including those described above. Information associated with your account will be kept until your account is deleted, unless we no longer need the data to provide products and services.”	Frequency	Data storage · Improper storage	Pro-app

Instagram	“But these Affiliates will honor the choices you make about who can see your photos.”	Agents and determinants	Data sharing · Improper access · Unauthorized secondary usage	Neutral
	“…may retain information (including your profile information) and User Content for a commercially reasonable time for backup, archival, and/or audit purposes.” “Instagram may modify or update this Privacy Policy from time to time, so please review it periodically.”	Frequency	Data storage · Improper storage Data collection, data sharing, and data storage	Pro-app Pro-app
	“This information would allow third-party ad networks to, among other things, deliver targeted advertisements that they believe will be of most interest to you.”	Relevant qualities	Data sharing · Unauthorized secondary usage	Neutral
Twitter	“When you share information or content like photos, videos, and links via the Services, you should think carefully about what you are making public.”	Agents	Data sharing · Improper access · Unauthorized secondary usage	Pro-app

	“If we make a change to this policy that, in our sole discretion, is material, we will notify you via an @Twitter update or email to the email address associated with your account.”	Claims	Data collection, data sharing, and data storage	Pro-app
	“We may share or disclose your information at your direction, such as when you authorize a third-party web client or application to access your account or when you direct us to share your feedback with a business.”	Determinants	Data sharing · Improper access · Unauthorized secondary usage	Pro-user
	“Twitter broadly and instantly disseminates your public information to a wide range of users…” “We may revise this Privacy Policy from time to time.”	Frequency	Data sharing · Improper access Data collection, data sharing, and data storage	Pro-app Pro-app
Snapchat	“Keep in mind that, while our systems are designed to carry out our deletion practices automatically, we cannot promise that deletion will occur within a specific time frame.”	Claims	Data sharing and data storage · Improper access · Unauthorized secondary usage · Improper storage	Pro-app

	"We may change this Privacy Policy from time to time… Sometimes… Other times…" "Outside of Snaps, the rest of our services may use content for longer periods of time, which means those services may follow different deletion protocols." "Or if you submit content to one of our inherently public features, such as Live, Local or any other crowd-sourced service, we may retain the content as long as necessary to offer and improve the services."	Frequency	Data collection, data sharing, and data storage Data sharing and data storage · Unauthorized secondary usage · Improper storage Data storage · Improper storage	Pro-app Pro-app Pro-app
	"What do we do with the information we collect? The short answer is: provide you with an amazing set of products and services that we improve relentlessly."	Relevant qualities	Data collection	Pro-user

Figure 2. Analysis of mobile apps' privacy policies language and user concerns

	Control mechanism	User privacy concern(s)	Control
Facebook	Activity Log Tool	Data sharing and data storage · Improper access · Improper storage	Pro-user

	Advertising Preferences	Data collection and data sharing · Improper collection · Unauthorized secondary usage	Neutral
	Deactivation/ Deletion	Data collection and data storage · Improper collection · Improper storage	Pro-user
	Privacy Settings and Tools	Data sharing · Improper access	Pro-user
	Timeline and Tagging Settings	Data sharing and data storage · Improper access · Unauthorized secondary usage · Improper storage	Pro-user
	Social Reporting	Data collection and data sharing · Improper collection · Unauthorized secondary usage	Pro-user
Instagram	Blocked Users	Data sharing · Improper access	Pro-user
	Comments	Data sharing · Improper access	Pro-user
	Edit Profile Option	Data collection and data storage · Improper collection · Improper storage	Pro-user

	Linked Accounts	Data collection and data sharing · Improper collection · Improper access · Unauthorized secondary usage	Neutral
	Private Account	Data sharing · Improper access	Pro-user
	Story Settings	Data sharing and data storage · Improper access · Improper storage	Pro-user
	Two-Factor Authentication	Data sharing · Improper access	Pro-user
Twitter	Account Settings	Data collection, data sharing, and data storage · Improper collection · Improper access · Improper storage	Pro-user
	Privacy and Safety Settings	Data collection and data sharing · Improper collection · Improper access · Unauthorized secondary usage	Pro-user
	Timeline Settings	Data collection · Improper collection	Neutral
Snapchat	Advertising Preferences	Data sharing and data storage · Improper access · Improper storage	Pro-user

	Blocked	Data sharing · Improper access	Pro-user
	Contact Me	Data sharing · Improper access	Pro-user
	Deactivation/ Deletion	Data storage · Improper storage	Pro-user
	Login Verification	Data sharing · Improper access	Pro-user
	View My Story	Data sharing · Improper access · Unauthorized secondary usage	Pro-user

Figure 3. Analysis of mobile apps' control mechanisms and user concerns

Discussion

There were several findings worth noting as commonalities throughout the mobile apps as the culmination of this research. One commonality of the mobile apps is that similar, if not exact, language was found in the policies. For example, all apps use the word, "Services," to reference offerings to users instead of specifically naming functions of the apps; such as the ability to comment, like, share, post, etc. The apps also share similar in-app features as control mechanisms. All apps offer options for deactivation/ deletion, advertising preferences, and privacy settings in accounts to assuage user privacy concerns. Although, control mechanisms are not named the same across apps.

Comprehensively, the privacy policy language of the mobile apps favor control towards the creators of the apps. The language mostly uses vague and broad terms that could leave users' still curious on the company's information-handling practices. Owners of these apps could have purposefully written policies in this manner to ease assignments and responsibilities to users. The policies do not discuss much of the payoff users will receive from the apps. Theoretically, users need to receive great personalization for relinquishing private information; current policy language does not reflect this argument. These unsure feelings on part of the user could lead to distrust, and ultimately, less use of the app.

The control mechanisms of mobile apps favor control towards the users of the apps. All of the in-app features give users levels of control over accounts in some form. Users with options to address concerns over data collection, data sharing, and data storage may feel more trust in the app because of the regulation these built-in functions give the user to handle her own concerns.

A user may feel comfortable surrendering more information to the app, for personalization, with these mechanisms. It is possible for more trust in the creator-user relationship to exist because of the feeling of more effort put in on part of the app with these control mechanisms. However, the combination of the language objectives and control mechanisms shows a compromise.

A constant negotiation exists in the relationship of creators and users. The implementation of the language and control mechanisms in the mobile apps demonstrate this negotiation. Creators use privacy policy language for liability purposes, and users have control mechanisms to protect privacy concerns on data collection, sharing, and storage. There is a constant tradeoff that companies want more information to better serve users, but users are unwilling to give information if it is not worthwhile. A unspoken balance must be achieved for a successful creator to user relationship.

Limitations

The research is limited in several aspects. A significant limitation of this discourse is that data was not original to this research, but taken from previous works to establish the argument. Users' privacy concerns are assumed to be universal based on other studies involving the Internet. A survey of users' demographics, interests, and habits referring to usage of mobile apps would have been more beneficial than building off of themes from other bodies of research, and applying those themes to examples of mobile apps.

Another limitation of this study is that research was only collected from four social network apps. This does not adequately represent findings in privacy policies of mobile apps, or the category of social network mobile apps. The study is only applicable to Facebook, Instagram, Twitter, and Snapchat. More social network mobile apps need to be combined with these four to draw conclusions suitable to the category of social networks. Also, a more inclusive examination would include numerous mobile apps from across categories, not only social network apps. Mobile apps should have been examined across iOS and Android operating systems, not only iOS, for the same reasons.

Other forms could have been looked at to strengthen the argument, as well. Only papers titled, "Privacy Policy," or, "Data Policy," from the companies of the mobile apps were viewed on the assumption that the content was most relevant to the topics. Papers generally titled, "Terms of Service," or "Terms of Use," could have gave slightly more insight on data-handling practices.

Finally, the control mechanisms in this paper are not a whole representation of control mechanisms that can be meet users' privacy concerns and the language of privacy policies. The control mechanisms were chosen on how well the mechanism could be applied to privacy concerns and the language of the policy. Users can take individual precautions outside of in-app features to mediate concerns, and these actions may or may not align with the language of the privacy policy. On language, certain words and phrases were pulled from the policies that represented the language characteristics for the argument well.

Conclusion

This body of research is the beginning of a more in-depth investigation into the privacy relationship through policy language and control mechanisms. Future research has the potential to analyze policy language to contribute to the language themes categorized in this study with new dimensions specific to mobile apps. The prior literature to discern these themes is dated; the requirements of creators and users of mobile apps, specifically social networking apps, have changed over time. The majority of policy language favors the app in terms of control over information; to effectively serve users the language needs to better reflect equity for the user.

This study should also account for user control mechanisms, or control mechanisms not offered as in-app features but actions users take to appease privacy concerns. For example, in terms of social media, the use of multiple email addresses or pseudonyms for accounts. An analysis on user control mechanisms would adjust the perspective of this research from creators' actions to meet users concerns, to users' actions to meet their own concerns. These factors allow for exploration of new arguments in language and control of privacy concerns.

The four mobile apps in this study help to understand policy language of mobile apps; control mechanisms of mobile apps; and how these elements pass control to creators and users of mobile apps. The material here gives insight into the relationship between creators and users, especially as it pertains to privacy. Policy language considers the demands of the apps over the users' privacy concerns; whereas in-app features support theses concerns overs the apps' desires for information. Both policy language and control mechanisms work cohesively to manage the relationship between creators and users.

The discussion of the relationship between creators and users of mobile apps warrants improvements for equity sake. Language should acknowledge users more than current policies, but this does not need to be reciprocated through in-app features since creators establish those mechanisms. Also, better communication, through email or in-app notifications would provide further awareness of resources to moderate users' privacy. An increase in tools and awareness would help to diminish privacy concerns in mobile apps, and strengthen the relationship between creators and users for harmonious exchanges of information.

References

Awad, N. & Krishnan, M. S. (2006, March). The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and The Willingness to be Profiled Online for Personalization. *MIS Quarterly.* (Vol. 30, No. 1, pp. 13-28).

Brown, M. & Muchira, R. (2004). Investigating the Relationship between Internet Privacy Concerns and Online Purchase Behavior. *Journal of Electronic Commerce Research.* (Vol. 5, No. 1, pp. 62-70).

Buchanan, T., Paine, C., Joinson, A., & Reips, U. (2007, January 15). Development of Measures of Online Privacy Concern and Protection for Use on the Internet. *Journal of the American Society for Information Science and Technology.* (pp. 157-165).

Chellappa, R. & Sin, R. (2005, April). Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma. *Information Technology and Management.* (Vol. 6, No. 2, pp. 181-202).

Clarke, R. (1999, February). Introduction to Dataveillance and Information Privacy, and Definition of Terms. *Communications of the ACM.* (Vol. 42, Issue 2, pp. 60-67).

Cranor, L., Reagle, J., & Ackerman, M. (1999, April 14). Beyond Concern: Understanding Net Users' Attitudes About Online Privacy. *The Internet Upheaval: Raising Questions, Seeking Answers in Communications Policy.*

Culnan, M. & Armstrong, P. (1999, February 1). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science.* (Vol. 10, pp. 104-115).

Data Policy. (2016, September 29). Retrieved April 14, 2017 from https://www.facebook.com/policy.php.

Eastlick, M., Lotz, S., & Warrington, P. (2003, November 3). Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of Business Research.* (Vol. 59, pp. 877-886).

Farnden, J., Martini, B., & Choo, KKR. (2015, May 12). Privacy Risks in Mobile Dating Apps. *In Proceedings of 21st Americas Conference on Information Systems.* (pp. 1-16).

Friedman, B., Kahn, Jr., P., & Howe, D. (2000, December). Trust Online. *Communications of the ACM.* (Vol. 43, No. 12, pp. 34-40).

Jain, A. & Shanbhag, D. (2012, July 18). Addressing Security and Privacy Risks in Mobile Applications. *IEEE Computer Society.* (Vol. 14, Issue 5, pp. 28-33).

Jenson, C. & Potts, C. (2004, April 24). Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.* (pp. 471-478).

Leontiadis, I., Efstratiou, C., Picone, M., & Mascolo, C. (2012, February 28). Don't kill my ads! Balancing Privacy in an Ad-Supported Mobile Application Market. *Proceedings of the Twelfth Workshop on Mobile Computing Systems & Applications.* (Vol. 2, pp. 1-6).

Li, Y. (2012, December). Theories in online information privacy research: A critical review and an integrated framework. *Decision Support Systems.* (Vol. 54, No. 1, pp.471-481). Look for diagram to model mine.

Lin, J., Amini, S., Hong, J., Sadeh, N., Lindqvist, J., & Zhang, J. (2012, September 5). Expectation and Purpose: Understanding Users' Mental Models of Mobile App Privacy through Crowdsourcing. *Proceedings of the 2012 ACM Conference on Ubiquitous Computing.* (pp. 501-510).

Malhotra, N., Kim, S., & Agarwal, J. (2004, December). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research.* (Vol. 15, No. 4, pp. 336-355).

Morgan, R. & Hunt, S. (1994, July). The Commitment-Trust Theory of Relationship Marketing. *American Marketing Association: Journal of Marketing.* (Vol. 58, No. 3, pp. 20-38).

Pollach, I. (2007, September). What's Wrong with Online Privacy Policies? *Communications of the ACM.* (Vol. 50, No. 9, pp. 103-108).

Privacy Policy. (2013, January 19). Retrieved April 14, 2017 from https://www.instagram.com/about/legal/privacy/.

Privacy Policy. (2017, April 12). Retrieved April 15, 2017 from https://www.snap.com/en-GB/privacy/privacy-policy/.

Sheehan, K. (2000, May 8). Toward a Typology of Internet Users and Online Privacy Concerns. *The Information Society: An International Journal.* (Vol. 18, pp. 21-32).

Sutanto, J., Palme, E., Tan, C. H., & Phang, C. W. (2013, December). Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users. *MIS Quarterly.* (Vol. 37, No. 4, pp. 1141-1164).

Twitter Privacy Policy. (2016, September 30). Retrieved April 15, 2017 from https://twitter.com/privacy?lang=en.

United States Department of Labor. Guidance on the Protection of Personal Identifiable Information. Washington, DC.

Viseu, A., Clement, A., & Aspinall, J. (2007, February 17). Situating Privacy Online: Complex Perceptions and Everyday Practices. *Information, Communication & Society.* (Vol. 7, pp. 92-114).

Wang, H., Lee, M., & Wang, C. (1998, March). Consumer Privacy Concerns about Internet Marketing. *Communications of the ACM.* (Vol. 41, No. 3, pp. 63-70).

Wang, Y.D. & Emurian, H.H. (2004, February 18). An overview of online trust: Concepts, elements, and implications. *Computers in Human Behavior.* (Vol. 21, pp. 105-125).

Wetherall, D., Choffnes, D., Greenstein, B., Han, S., Hornyack, P., Jung, J., Schechter, S., and Wang, X. (2011). Privacy Revelations for Web and Mobile Apps. *The Advanced Computing Systems Association.* (pp. 1-5).

Xu, H., Gupta, S., Rosson, M., & Carroll, J. (2012, December 14). Measuring Mobile Users' Concerns for Information Privacy. *AIS Electronic Library.* (pp. 1-16).

Yang, J., Yessenov, K., & Solar-Lezama, A. (2012, January). A language for automatically enforcing privacy policies. *ACM SIGPLAN Notices - POPL '12.* (Vol. 47, Issue 1, pp. 85-96).

Zhou, Y., Zhang, X., Jiang, X., & Freeh, V. (2011). Taming Information-Stealing Smartphone Applications (on Android). *Trust and Trustworthy Computing. Lecture Notes in Computer Science.* (Vol. 6740, pp. 93-107).