UCLA

UCLA Electronic Theses and Dissertations

Title

The Datafication of Mindfulness: Big Data, Mental Health, and the Perception of Privacy

Permalink

https://escholarship.org/uc/item/60p8n6bn

Author

Gant, Lindsey Kathleen

Publication Date

2018

Peer reviewed|Thesis/dissertation

eScholarship.org Powered by the California Digital Library University of California

UNIVERSITY OF CALIFORNIA

Los Angeles

The Datafication of Mindfulness:

Big Data, Mental Health, and the Perception of Privacy

A thesis submitted in partial satisfaction of the

requirements for the degree

Master of Library and Information Science

by

Lindsey Kathleen Gant

2018

© Copyright by

Lindsey Kathleen Gant

2018

ABSTRACT OF THE THESIS

The Datafication of Mindfulness:

Big Data, Mental Health, and the Perception of Privacy

by

Lindsey Kathleen Gant

Master of Library and Information Science

University of California, Los Angeles, 2018

Professor Christine L. Borgman, Chair

Americans increasingly turn to mobile applications to promote health and wellness in their lives. These applications provide mobile tracking and self-regulatory tools that allow users to monitor their own mental health. Categorically known as mindfulness applications, they help manage stress, anxiety, and depression, and promote productivity and build healthy habits. Mindfulness applications collect and retain highly sensitive, personal information regarding users' mental health, habits, and self-regulatory behaviors. This thesis addresses the perceptions of mindfulness practitioners about data collection practices and privacy within these applications. It examines the perceived benefits of using these applications, the extent to which practitioners are aware of these data collection practices, and the level of concern they have for their data privacy.

Keywords: Big Data, Mindfulness, Privacy, Consumer Rights, Smartphone Applications

The thesis of Lindsey Kathleen Gant is approved.

Jonathan Furner

Leah A. Lievrouw

Christine L. Borgman, Committee Chair

University of California, Los Angeles

2018

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

This thesis would not be possible without the help of some very important people. First of all, a big thank you to the staff at UCLA FITWELL, especially Kelly Shedd and Isabelle du Soleil, for allowing me to briefly interrupt their Yoga classes so that I could recruit for this project. Their time and patience are very much appreciated. I also would like to thank my thesis committee, Professor Jonathan Furner, Professor Leah Lievrouw, and Professor Christine L. Borgman, for offering their support and expertise to this project. Without their encouragement, I likely would not have chosen the thesis option for this program. I specifically want to thank Professor Borgman for her mentorship and inspiration throughout this process. I am incredibly proud of this final product and it is purely because of her guidance that I managed to get to this point. Finally, I would like to thank the students that took the time to speak with me for this project. They are the primary reason for pursuing this project; I hope it helps to pave the way to protect their privacy and consumer rights in the future.

THE DATAFICATION OF MINDFULNESS

Big Data, Mental Health, and the Perception of Privacy

The collection of personal data is ubiquitous for smartphone applications. It contributes to the expansive network of Big Data and the economic structure that facilitates data transmission, sharing, and usage. Privacy advocates express concern over the collection of personal data due to its potential infringement of consumer rights, depending upon the type of information that modern tech devices track, collect, and share, as well as the extent of user awareness of the usage of their data in this manner. This thesis addresses these problems as demonstrated through Mindfulness Smartphone Applications. These mobile applications allow users to track elements for purposes of self-regulation related to their mental and physical health, including their mood, emotions, and behavior. Despite the sensitivity of this information, mindfulness applications fall outside the scope of regulations by the Health Insurance Portability and Accountability Act (HIPAA).

Mindfulness reflects an important and valuable area of study specific to data privacy, yet little research or analysis exists on this subject. In general, previous discussions regarding these privacy concerns relate to the broad scope of health and wellness applications, specifically those that allow users to track and monitor their physical activity or biometric data. Applications that promote the self-regulation of mood, emotions, and behavior are generally included under this wide umbrella of wellness applications, however it is extremely important to differentiate applications that track mental health from those that track physical health. This distinction is not typically made within discussions about privacy concerns with self-help applications. Through mindfulness applications, data collected about mental health and activities related to self-regulation becomes a commodity for big business, putting privacy and user control over their personal data at stake.

The companies that employ data collection practices within mindfulness applications make mental health data a commodity that is sold to advertisers for a commercial profit. Advertisers exploit this data to target consumers for products and services relating to the mental health issue. The data also categorize people into commercialized networks based upon mental that might later be accessible by insurance companies and future employers. The extreme personalization of these applications enhances the sensitive nature of the information logged and tracked within them. This thesis examines the perceptions of privacy by mindfulness practitioners to determine the extent to which they are aware of these practices and, in turn, if they have concerns because of this awareness.

In general, mobile smartphone applications store information about users, whether the software automatically track this information within the device or if the user inputs information manually into the application. Companies collect these personal data for purposes such as sales and advertising, personalization and customization, and software analytics. This thesis will reflect upon the consumer repercussions of these pervasive data collection practices for mindfulness applications in the United States.

Relevant Terms

There are two important terms that I often reference in this analysis that I believe should be defined and explained before delving into the background for this study: Mindfulness and the Self-Regulation Theory.

Mindfulness

Mindfulness is the practice of complete awareness of one's own thoughts, mood, behavior, and emotions. Mindfulness practitioners often regard this practice as a therapeutic technique meant to retain control over the self and to be actively engaged with the internal response to external forces. These forces might include interactions with other people, experiences, personal hardships, or one's own physical needs. According to the American Psychological Association (APA), empirical research supports the practice of mindfulness to reduce rumination resulting from depression, stress, anxiety, and emotional reactivity, and enhance the working memory, focus, cognitive flexibility, relationship satisfaction, and "self-insight, morality, intuition and fear modulation" (Davis & Hayes, 2011).

Mindfulness originates from Buddhist practices of meditation; however, Jon Kabat Zinn introduced the American interpretation of this practice in 1979. He founded the Stress Reduction Clinic at the University of Massachusetts Medical School in which he created the Stress Reduction and Relaxation Program, later renamed as the "Mindfulness-Based Stress Reduction" program (Shea, 2018). The last decade witnessed a dramatic increase of interest in mindfulness and meditation in America. According to a study by Van Dam et al, the number of media newspaper articles that use the term "mindfulness' or 'meditation' increased by 3% percent and the number of original scientific articles in journals increased by 6.6% (Van Dam et al., 2018). As a result, the hype around mindfulness and meditation shifted beyond the news media towards technological tools that can help individuals track their own habits and behaviors as a mechanism to self-regulate and enhance their own mental wellness. The large number of mobile applications that allow users to easily track and reflect upon their own self-regulatory behaviors represent this technological shift. Psychologists and therapists accept mindfulness as a therapeutic method for mental health conditions, called Mindfulness Based Cognitive Therapy (MBCT). According to Grossman et al and Khourey et al, Mindfulness Based Stress Reduction (MBSR) is "moderately effective in reducing stress, depression, anxiety and distress and in ameliorating the quality of life of healthy individuals" and "may help a broad range of individuals to cope with their clinical and nonclinical problems"(Grossman, Niemann, Schmidt, & Walach, 2004; Khoury, Sharma, Rush, & Fournier, 2015).

Self-Regulation Theory

Self-regulation is not a new concept inherent to mindfulness or meditation. In 1991, Albert Bandura wrote the "Social Cognitive Theory of Self-Regulation", in which he states that "people motivate themselves and guide their actions in an anticipatory proactive way" (Bandura, 1991). Self-regulation is defined as an individual's ability to monitor and evaluate their own motivations and behavior, while reflecting upon their "own performances, the conditions under which they occur, and the immediate and distal effects they produce"(Bandura, 1991, p. 250). This individual might pay particular attention to their mood as a factor in relation to their own behavior, and their act of self-regulation and self-monitoring may lead to self-diagnosis by reflecting upon the patterns that emerge from their documentation (Bandura, 1991). According to Friese and Hofmann, there is evidence to support the relationship between mindfulness and self-regulation, exemplified by the process of healthier eating. A thoughtful relationship to eating indicates that an individual is aware of their bodily needs in order to prevent binge eating or emotional eating due to their increased awareness of their mental state and their own psychological responsiveness to ingesting food (Friese & Hofmann, 2016). This connection between mindfulness and self-regulation is at the core of the purpose and usefulness of mindfulness applications. The application design promotes self-regulation by supporting digital tools that allow users to track their behavior and mental state for a wide variety of purposes, allowing them to quantify and assess their data trends over time. In a mobile application dedicated to mindful eating, these tools might include a calorie counter, a timer in which the user is reminded to eat, or generally assist them with determining their overall satisfaction with that meal to build and maintain healthy habits for weight loss or overall physical and mental wellness. The application *Am I Hungry?*, labeled as a Mindful Eating Virtual Coach, for example, helps users to “make more conscious decisions about why, when, what, how, and how much you eat, and where you invest your energy” (“Am I Hungry?,” 2018). This form of application appeals to users who are looking to become more actively aware and in tune with the process of eating as a function of wellness.

LITERATURE REVIEW

This study draws upon previous research about data collection practices in mobile smartphone applications and correlating concerns about privacy. Specifically, I investigate the processes in which personal data are collected within applications, including tracking practices imbedded within the application software about specific usage patterns, including geolocation, and the ways in which this data is shared or sold to third-party companies for the purposes of targeted advertising. I also analyze the current regulations of these practices to determine the barriers to regulation that mindfulness applications currently have. Overall, I discuss important elements that relate to the perception of data collection practices, the perceived benefits to using these applications, the level of awareness users have about these processes, and the amount of concern users feel about data collection practices and policies. I represent these areas through a discussion on datafication, self-regulation, and personalization within these applications and offer a critique of user interaction and their understanding of privacy policies.

Data collection practices in mobile applications

Mobile Applications, in general, collect and store a great amount of information about the users who install this software on their smartphones. It is important to understand what these apps have the capability to collect to fully understand the stated problem of mindfulness apps. For the purposes of this paper, I will analyze the issues that affect both Android and iOS devices to demonstrate the overarching value of this discussion.

Application Permissions

When users download an application, there is typically a series of permissions that they must approve in order to proceed. These permissions identify how the apps connect to the smartphone's hard drive, including such actions such as: read and modify contents; full-network access; access to camera or microphone; send SMS messages. The term 'access', found within these permissions, refers to the ability of the application software to read the content stored on the smartphone device, including the usage of the internet through the device or the ability to interact with other software already installed on the device, such as the calendar or the microphone. While these permissions are extremely important for recognizing the extent of access an app might have to a user's personal device and network, these permissions tend to be vague and easily overlooked by those initially interested in downloading the app. According to Katie Shilton, one of the problems with app permissions is that they are made available to the user only after they make the decision to download the app (Shilton & Greene, 2017). There should be a redesign of application permissions such that users know exactly how their information will be used at the same time as, or before, making this decision, especially since in many instances, the permissions may be the only way in which users reflect upon the ways in companies manage and collect their data.

Third-Party Access

Mobile application companies often state in their privacy policy that their aggregate data may be shared with third-party sources for advertising, marketing, analytics, and software development. These third-parties may track and collect information about mobile application users with their own tools, including: cookies, web beacons, software development kits (SDKs), and other such technologies. However, a major problem with this is that these companies list the ways third-party companies collect information, but they do not state who these third-parties are and the ways in which they are using the information. It is typical of app developers to state that these companies have access to this data, but they are not lawfully obligated to control what these third-parties do with this information. According to Mayer and Mitchell, there are various problematic and potential harmful instances that may happen regarding third-party access to collected information: “The third party is also a first party”; “The first party sells the user’s identity”; “A first party unintentionally provides identity”; “The third party uses a security exploit”; and “Re-identification” (Mayer & Mitchell, 2012). It is important for the user to understand who the first-party ownership of their data belongs to, noting the company and any affiliates attributed to it, and which third-parties have access to this information before the user can make a properly informed choice regarding whether to download the application. As it stands, if this information is not provided, this choice is not a valid option for the user.

Current Regulation of Health/Wellness Applications

There is greater regulation and control over the legality of health and wellness applications in the American legal system in comparison to mental health or mindfulness. Three major entities determine whether certain heath applications must adhere to stricter laws governing the collection of patient medical data: The Federal Trade Commission (FTC), the Food and Drug Administration (FDA), and the U.S. Department of Health and Human Services (HHS). The important legislation of note that polices health data collection is the Health Insurance Portability and Accountability Act (HIPAA), the Federal Food, Drug, & Cosmetic Act (FD&C Act), the Federal Trade Commission Act (FTC Act), and the FTC's Health Breach Notification Rule ("Mobile Health Apps Interactive Tool," 2016). Applications that are covered by HIPAA, in particular, typically apply to covered entities, such as health care clearinghouses or health care providers, or business associates, which are groups that create an app on behalf of one of these covered entities (("Health App Use Scenarios & HIPAA," 2016)). The FDA, however, "recognizes the extensive variety of actual and potential functions of mobile apps, the rapid pace of innovation in mobile apps, and the potential benefits and risks to public health represented by these apps" (("Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff," 2015). While their focus of regulation is more specific to explicit applications used a medical device, for example, a device that can be used to track electrocardiograph results, their 2015 Guidance for Mobile Medical Applications proposes many instances in which the FDC will exercise enforcement discretion. According to the FDA, these apps, that may be “intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease” are of lower risk to the public but may still contain compromising data for the application users (“Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff,” 2015) While most medical-related applications are not legally required to adhere to the aforementioned laws, as entities not explicitly linked to the health care industry promote them, they receive much more scrutiny to the data collection policies than any other form of mobile application, despite the category of information they are collecting.

Current Regulation of Mental Health Applications

For this paper, mental health refers to an individual’s psychological wellbeing, including emotional stability, thoughtful clarity, self-actualization, and overall satisfaction in the events and relationships in their life. Mental health smartphone applications encourage self-regulation to promote positive behaviors to maintain mental wellness. These applications, however, do not have any form of legal regulation that are similar to the laws enforced for health or wellness medical devices, despite the many similarities between the sensitive nature of the collected data. There is little research or discussion about privacy and mobile mental health applications, let alone legal regulation over such issues. In some instances, such as with health-related applications, HIPAA dictates policies regarding the release of personal mental health data but only for applications that are a direct source of communication between the user and the mental health services provider (“HIPAA Privacy Rule and Sharing Information Related to Mental

Health," 2017). Beyond this scope, there is very little additional regulation of personal mental health information about individuals.

Datafication of Self-Regulation

The advent of Big Data over the last two-decades is manifest in all aspects of the modern world, including the institutions of healthcare, government, public policy, entertainment, and education. The purpose and intent of this tool is to collect and organize data about people and institutions into large data sets that may be examined and evaluated to determine trends and patterns of and about human behavior. The industry around Big Data, from the big corporations such as Google and Amazon who collect digital data, to industry analysts and data brokers, has become extremely lucrative, such that the market revenue has increased by 600% since 2011, and is projected to be roughly $56 billion by 2020 (("Global big data industry market size 2011-2027 | Statistic," 2018). As is stated with the now well-known cliché, data is the new oil, due to the abundance and ubiquity of data that permeates the new global data-driven economy ("The world's most valuable resource is no longer oil, but data," 2017).

Datafication acts as a mechanism for the driving forces of Big Data. According to Ruckenstein and Schüll, there was a "data paradigm shift, typically by focusing on particular cases of 'datafication,' or the conversion of qualitative aspects of life into quantified data" (Ruckenstein & Schüll, 2017). According to van Dijck, "Datafication is a legitimate means to access, understand and monitor people's behavior is becoming a leading principle, not just amongst techno-adepts, but also amongst scholars who see datafication as a revolutionary research opportunity to investigate human conduct"(2014). Datafication is at the center of mobile smartphone applications that promote user self-regulation in terms of their physical and mental health. These tools reflect systems of personal informatics that allow users to collect and reflect upon personal information (Li, Dey, & Forlizzi, 2010). They allow users to log, track, and view any progressions or trends regarding their habits or behavior. In this way, "people participate in both the collection of the behavioral information as well as the exploration and understanding of that information" (Li et al., 2010). These applications encourage users to take an active role with the collection and transmission of their data by either uploading their information directly into the service or allowing trackers to automatically collect data transmitted by the smartphone device. Datafication encourages the measurement, manipulation, and monetization of human behavior, through the lens of the smartphone (van Dijck, 2014).

Datafication also allows Big Data organizations to create profiles for individuals based upon behavioral patterns and trends as determined by their collected data. They group and categorize these profiles, creating a network of users based upon their digital usage habits and their tracked data. Big Data promotes predictive policies for the purposes of targeted advertising based upon purported or supposed interests. The Federal Trade Commission critiques these predictive policies because of the potential usages of these categories beyond targeted advertising. In the 2016 FTC Report, there are expressed concerns of collected data used to target individuals for hiring pools:

> [The data broker] Spokeo assembled personal information from hundreds of online and offline data sources, including social networks, and merged that data to create detailed personal profiles, including name, address, age range, hobbies, ethnicity, and religion, and marketed these profiles for use by human resources departments in making hiring decisions (Federal Trade Commission, 2016).

Similar to concerns regarding the usage of these collected data for categorizing people for hiring purposes, there are concerns about predictive analytics for health care, including treatment options health care approval. The data collected through mobile smartphone applications typically fall outside the scope of HIPAA guidelines. HIPAA only regulates and controls the privacy and confidentiality of patient data through digital tools that is directly transmitted between patients and their health care professional, including any business affiliates (Glenn & Monteith, 2014). The same protections are in place for the sharing of personal data between the patient and their health insurance company.

Personalization

The level of personalization depends on the application's context and purpose and generally encompasses a large and complex system of personalization that is at the core of any conversation around privacy and technology. For the purposes of this discussion, I will focus on the Personalization-Privacy Paradox, Location-Based Services, and Targeted Advertising.

Personalization-Privacy Paradox

The critical debate regarding data collection for mindfulness applications relates to the Personalization-Privacy Paradox: the idea that in order for companies to offer personalized services though these applications, including the storage and retrieval methods for data saved in the app that allows for increased customization of the product or service, there is an inevitable trade-off with personal privacy and control over users' personal data (Sutanto, Palme, Chuan-Hoo Tan, & Chee Wei Phang, 2013).

Researchers argue that users are more willing to forgo their privacy rights in exchange for the benefits of increased personalization (Hann, Hui, Lee, & Png, 2002). According to Zhan Liu et al (2014), these decisions regarding the exchange of privacy are the result of a cost-benefit analysis, such that users must assess the perceived maximum benefit of "disclosing personal information, while minimizing the expected harm that may come from disclosing it" (Z. Liu, Shan, Bonazzi, & Pigneur, 2014). Liu states that this decision is based primarily upon the context in which the personal information is requested and may be correlated to the level of trust consumers have in the application service provider. Liu also states that the factors that are likely to increase the rate to which consumers provide personal information to the application service provider are *benefit belief*, or the perceived understanding that the service provider will secure their information in exchange for increased application personalization, *confidence and enticement beliefs*, or the trust that these providers are subject to legal standards to ensure the safety of their information, and *perceived usefulness*, in which consumers are more willing to exchange privacy for a service that boosts their performance in a certain area; in contrast, consumers are less likely to provide personal information due to *risk belief*, or the perceived risk or disclosing this information (Z. Liu et al., 2014).

Logging and Tracking

Oftentimes, for those working to become adept at a new skill, it is useful to keep track of the time spent practicing that skill and record any information about their mindful behaviors in order to reflect upon the trends in their practice over a period of time. Logging and tracking are preferred self-regulatory behaviors to promote habit formation in adherence to the pursuit of personal goals. This process includes "setting goals, planning, self-monitoring, and reviewing progress" over time (Kliemann et al., 2017). It is important to note the difference between tracking and logging: a tracking mechanism on a smartphone application does the work of monitoring activity levels for the user; it determines how long they spent using the application for a specific activity, including meditation timers or applications with guided meditations for the user to listen and engage with, as well as location and movement trackers to determine how long the user participates in a certain activity. Logging, on the other hand, is user monitored and controlled, in which they input information to the application about their activities, such as length of time meditating, their mood that day, or what food they eat for every meal. The difference between tracking and logging is the amount of control the individual has over data collection within the application.

Location Sharing

The trend towards increased personalization within smartphone applications is the collection of user location; this may be intended specifically to enhance the quality and Location-Based Services, or services that depend on the contextual location of the user to function, such as Maps, Weather, Shopping, etc., but the developer can choose to also collect this information in order to have an increased understanding of who their primary user base is, where they are located, and the contexts in which they use the application. Generally, cell towers, GPS, or the device's network connections help pinpoint the user's location and the application collects and transmits this information back to the developer. Application developers are often criticized for the collection of location information about its users without demonstrating explicit purpose for this collection. According to Werner, the extent to which developers collect location-based information should be limited, because "once such a system is successful and collects more and more users, it will not be able to guarantee for the privacy protection of the data" (Werner, 2016). Location-Based Services is an important topic in relation to mindfulness and wellness applications because there are often times in which location-services track user movement or might use this location information for targeted advertisements with a specific contextual relationship to that user. Location information, in general, reveals incredibly sensitive information about people, their activities, and their personal network (Herrmann, Hildebrandt, Tielemans, & Diaz, 2016). According to Herrmann et al, "location data reveals information about users that is potentially sensitive, difficult to anonymise, and entities with access to accurate location data are able to make inferences about, for example, home/work address, income level, religious beliefs, sexual preferences or health issues" (Herrmann et al., 2016, p. 146). There are various ways that users might attempt to mitigate the collection of their location data, including turning off Location Services on their devices or turning off location permissions for individual applications, however this method is generally "opt-out", meaning the individual must be aware of these practices and have enough concern about the collection to decide to remove the location-collecting mechanisms.

Targeted Advertising

The increase of technologies that embrace targeted advertising to fund their services is directly related to enhanced personalization within these technologies. Targeted (or behavioral) advertising is the act of taking information collected about individuals and using it as the basis to target goods and services to that person. The more that the developer knows about each user, including location, web browsing behavior, consumer habits, social networks, etc., the more tailored advertisements can be for that user. To have a deeper understanding of who this user is, the application developer might integrate with Google or Facebook, to connect directly to a strong indicator of the user's personal preferences and behaviors (Y. Liu & Simpson, 2016). According to Liu et al, this mode of targeted advertising reflects the Personalization-Privacy Paradox: "To enjoy useful services—using free applications, obtaining various coupons, tracking interested products and so on—many users choose to compromise: they provide personal information to advertisers (actively or passively), while maintaining that privacy is important to them" (Y. Liu & Simpson, 2016, p. 1659). One area of concern for privacy advocates is the usage of targeted advertising relating to sensitive information obtained through tracking user behavior on the web, including health and sexuality. The common anecdote that reveals this problem is the situation in which Target revealed the pregnancy of a teenage girl to her father because of behavior tracking and targeted advertising (Hill, 2012). Similarly, there is concern that individuals with mental health concerns will begin to see targeted advertisements for antidepressants. Targeted advertising, based upon sensitive and personal information, reflects a major area of concern for this thesis.

Usefulness of Privacy Policies

The Privacy Policy is one of the most important and fundamental documents that connect application developers to their users to communicate the extent to which user data is shared, sold, and protected in order for the user to be informed and educated about these policies unique to each company. While there is a long history related to the legality of Privacy Policies, the primary players in the enforcement of these policies are the Federal Trade Commission (FTC) and the California Online Privacy Protection Act of 2003 (CalOPPA). The FTC offers a succinct list of Best Practices that a company might follow to implement data security, including building a privacy policy that clearly displays what information is collected and how it is used ("Mobile Health App Developers," 2016). These guidelines help application developers build privacy and security into their design, by promoting data collection minimization, transparency, accessibility, and lawfulness. It is important to remember, that these are simply guidelines and not law;

although they also help developers adhere to the FTC Act, which prevents “deceptive and unfair” acts against consumers (“Federal Trade Commission Act,” 2013). CalOPPA, however, legally requires websites and online services to have a privacy policy if they collect any private user information. According to the California Department of Justice, even though this law applies solely to the Personally Identifiable Information of California Residents, the economic importance of the users found this this jurisdiction widely affects app developers across the country, enforcing widespread acceptance of the inclusion of a privacy policy (Harris, 2014). In the United States, consumers must be notified about any policies, or changes to these policies, regarding the usage of their personal information, so that they might make a rational decision to either accept these terms or to cease using the service (Reidenberg, 2015).

Privacy Policies and Consent

The privacy policies dictate the level of awareness that users have about data collection practices in their applications. Despite the availability of these privacy policies, there is reason for concern regarding the usefulness of these policies or if they are even read or understood by the average smartphone application user. According to Reidenberg et al, there is an inherent problem with the United States’ “Notice and Choice” framework: there is an assumption that there is an equity among all consumers of the ability to read and understand the legal framework around privacy policies to the extent that they are able to sufficiently consent to the binding agreement denoted within the policy (Reidenberg, 2015). The Reidenberg et al research study compared the comprehension level of privacy policies between average (layman) consumers, knowledgeable users, and experts. Their findings demonstrate the following issue: “…privacy policies are written ambiguously and in a way that leads both knowledgeable users and crowd workers to misapprehend websites’ data practices as well as cause disagreement among experts with respect to certain data practices” (Reidenberg, 2015, p. 87). This study demonstrates the overarching concern with the understandability of legal documents for users to make the decision to use the service under the stipulations presented in the policy.

Similarly, there is debate over whether or not the average user reads the Privacy Policy before agreeing to use the service or application. There is evidence to show that these policies are often ignored, either due to the lack of concern by the individual, little accessibility of the policy to the user, or the context in which the policy is presented. One research study employed “eye tracking methodology” to determine if the policies are being read within the online context (Steinfeld, 2016). In this study, only around 20% of the participants actively clicked the provided link to view the Privacy Policy compared to the 80% who agreed to the terms and conditions without reading the provided legal documents. However, among the group that did select to view the privacy policy, users were more likely to read the policy in its entirety if supplied to the user by default, while the remainder of the participants did not read the policy carefully or to completion (Steinfeld, 2016). It is important to question the validity of the “notice and choice” policy in America, in terms of full user comprehension of the data sharing policies to which they agree. Privacy advocates largely debate this policy, in general, because it places the responsibility over data sharing on the consumer, rather than on the companies that collect their data. By questioning the extent to which consumers read the privacy policies, it shifts the blame for the consequences of this data collection onto the consumer rather questioning the merit and validity of these policies in the first place.

User Awareness

There are varying ways in which users may become informed about data collection practices through their smartphone devices: privacy policies, application permissions, and mass media. As previously noted, there is question if privacy policies are successful in dictating data collection practices to the user, if they are understandable, or if they are actually read by the user. Application permissions, on the other hand, are directly integrated into the application download process. The user must actively agree or disagree to the permissions before the download can begin. These permissions may include: access to contacts, calendars, full network access, location, etc. Users are more likely to have some level of information about these practices as determined through the permissions, rather than the privacy policy, however permissions are extremely limited in the information presented to the user about what user data is collected and how that information is shared to third-party sources. According to Tsavli et al, "there is a tendency of users and developers to unsubscribe from security awareness related actions; the former could be due to fatigue of the consecutive acceptance of more and more permission requests and the latter due to the high complexity of the permissions model" (Tsavli, Efraimidis, Katos, & Mitrou, 2015). In addition to application permissions, the extent to which users are aware of data collection practices may be determined through mass media, as well as any trending news stories about data breaches. These events may trigger mass interest in the information collected through these applications, leading to more informed understandings of the ways in which personal information is shared. This does, however, cause confusion over the difference between data security and information privacy.

It is surprisingly difficult to find relevant research regarding the level of awareness users have about data collection practices in smartphone applications, beyond analysis and critique of privacy policies in general. This may be an additional area for future research.

Perception of Anonymity

In general, people are more willing to share personal data if it is collected in an anonymized aggregate that is not tied to their personal identity (Gustarini, Wac, & Dey, 2016). Privacy Policies for mobile applications often describe the difference between personally identifiable information (PII) or aggregate information that is not tied to the user's PII. However, according to Patrick Tucker in the 2013 MIT Technology review, "the more data there is, the less any of it can be said to be private, since the richness of that data makes pinpointing people 'algorithmically possible'" (Tucker, 2013). With the increased number of data points collected in the ever-expanding network of Big Data, it is important to question the validity of anonymity and if it is possible for a user to be anonymous in their mobile interactions in the modern age. Similarly, according to Gustarini et al, even though the information itself may be anonymous, the context information about the action itself may give insight into the personal routines and behaviors about that individual (Gustarini et al., 2016). While users might prefer anonymity in their online activities, it is important to determine the veracity behind this claim and if what users perceive to be anonymous is actually anonymous.

METHODOLOGY

The purpose of this study is to explore the perceptions of privacy from the perspective of mindfulness practitioners. This study seeks to address the following research questions:

1. What are the perceived benefits of using mindfulness smartphone applications?
2. In what ways are mindfulness practitioners aware of data collection practices in these applications?
3. What influences the levels of concern that mindfulness practitioners have about data security and privacy of data collected and shared by corporations and their affiliates?

Through a series of interviews, it is possible to determine the range of attitudes and perceptions about the levels of awareness and concern related to these practices.

IRB Submission

As a requirement to conduct research with human subjects at UCLA, I submitted a project proposal to the Institutional Review Board. Through this process, I ensured confidentiality and security for my interview participants due to the sensitive nature of the information they reveal during our conversations. The Review Board expedited this project due to its limited potential for harm to these participants. I submitted an amendment to this original proposal in order to alter my participant recruitment method, as I believed a direct email to potential volunteers would enhance the response rate for this project, however this method yielded little results.

Sample

I worked directly with the UCLA FITWELL program to recruit Yoga participants for a potential interview session in which they would reflect upon their usage of mindfulness applications, if they choose to use them, as well as their level of concern, if any, related to personal data collection practices. This program works with students, faculty, and staff to “make healthy lifestyle choices specifically in the areas of fitness and exercise, nutrition and weight management, stress management, and general health education” (“UCLA Recreation - FITWELL,” 2018). As part of this program, UCLA affiliates may purchase a Yoga Pass, which allows them to attend unlimited Yoga classes provided through FITWELL during the academic quarter. I specifically recruited participants through this program to ensure that the potential interview subjects practiced a form of mindfulness at least once (i.e. even if that day of recruitment was the student’s first attempt at practicing yoga as mindfulness). The class that I primarily attended for recruitment was titled “De-Stress: Yoga and Mindful Meditation” with the intent to find students and faculty who not only practiced Yoga for the physical fitness aspect of the activity, but those who were generally more interested in mindful intentionality for mental health. The second class I attended was titled “Yoga Flow and Meditation” to also recruit potential participants interested in mindful meditation.

At the beginning of each of class session, I gave a brief introduction to the study, describing its purpose and intent, before distributing recruitment flyers to interested volunteers. Each volunteer completed the required information on the flyer, that included name, email, UCLA status, and their usage level of applications for mindfulness or wellness. I then used this information solely to contact the student to schedule a future interview.

Participants for this project included nine UCLA students (graduate and undergraduate) and one faculty member, or ten participants in total. Of the final sample, eight of these students identified as female and two identified as male. Five were undergraduate students, four were graduate, and one was a faculty member. Each participant met with me for a scheduled interview in either a reserved campus study room or in a private office at their convenience. The interview would last between 20-45 minutes, in which I led a semi-structured discussion session relating to the reasons why they are interested in mindfulness, how technology enhances (or does not enhance) their mindfulness routine, and whether or not the privacy policy impacts their decision to use and/or input their personal information into their mobile phone application of choice.

One limitation of this sample is the gender distribution between male and female participants. I presume that most of Yoga Pass holders are female, based primarily on perceived attendance levels in the classes that I attended. A second limitation is the small number of interview participants. There was some difficulty with the recruitment process as it is difficult to get volunteers to agree to a scheduled 30-minute interview within their already busy class schedule. Recruitment was also limited to the rate of student attendance for the Yoga classes; this research project began near the end of Winter quarter, in which class attendance was low, and was also impacted by Spring Break, before class sizes increased at the beginning of Spring quarter. That said, the interview responses, as noted in the Findings section of this paper, demonstrate a breadth of responses that reflect the many important perspectives by consumers regarding their attitudes towards the data collection practices of mindfulness smartphone applications.

Procedure

The data collection occurred in March and April 2018. I conducted one thirty-minute interview each with the research participants (this interview length varied depending on the amount of detail the interviewee provided within their responses). I first began by obtaining informed consent by the participant: this consent form explicitly protects confidentiality of the participant's personal information and any sensitive information provided in their responses, especially due to the potential discussion relating to mental health and personal wellness within the interview. At the participant's agreement, I also recorded each interview using a personal digital recording device, to review and transcribe at a later date, in addition to the handwritten notes that I took during the interview.

The interview was semi-structured, as I had previously prepared list of questions to guide the discussion (found in Appendix A of this paper), however I encouraged a natural flow to the conversation to reassure and inspire the interviewee to either expand further about their perceptions on mindfulness or data collection practices, or to offer new and unexplored ideas relating to this topic. At the completion of each interview, I documented any important or relevant information that I learned through that interview or I noted any areas that needs further research. I also transcribed the areas of note from the recorded interview and coded the transcript with relevant keywords or phrases to label, sort, and analyze collected interview data.

FINDINGS

This section draws upon the interview responses from this research project to determine the overarching beliefs and perceptions about the data collection practices within mindfulness applications. I grouped their responses based upon my research questions to reflect on the perceived benefits of these applications, the extent to which mindfulness practitioners are aware of data collection practices, and their correlating level of concern for these practices. The participant responses varied widely regarding their level of awareness and concern, however they each demonstrated a thoughtful cost-benefit analysis regarding the continued usage of these applications. This section reflects upon their thought processes with examples directly from the interview responses.

It is important to note that many participants equated physical fitness and general activity to mindfulness and a form of meditation. They perceive physical activity to reflect mental health and clarity in the same way that meditation might provide. Therefore, while many of the applications discussed were explicitly mindfulness and meditation applications (i.e. *Calm*), others related more to the category of Health and Wellness (i.e. *MyFitnessPal*). I chose to include these apps within the interviews, as well, when the participant discussed them in relation to mental health and mindful self-reflection.

RQ1: What are the Perceived Benefits to Using Mindfulness Applications?

Individuals often choose to download and incorporate mindfulness applications into their daily routine for a variety of reasons. Mindfulness, as promoted through popular culture, might bring happiness to one's life by helping to enhance mental clarity and emotional wellness. These applications offer the ease and simplicity for the self-regulation and tracking mechanisms that are useful for habit formation. They play an important role in the lives of mindfulness practitioners, granting them insight to their own behaviors and patterns.

Mental Health

The practice of mindfulness directly correlates to mental health. Self-control, active engagement with one's thoughts and mental wellness, and positive engagement with others are all perceived benefits that the subjects of this study strive for through mindfulness. Psychologists substantiate the correlation between mindfulness and mental health and their promotion of mindfulness for traditional therapeutic routines. Participant 2 of this research study, for example, reflected upon his own experiences while in group therapy for depression, noting that mindfulness was often encouraged, though it wasn't until after completing his group sessions that he began to explore mindfulness in his own life. The subjects within this study demonstrated this mental health correlation through their perception of how they define mindfulness, the purposes for why they practice mindfulness and, in turn, if they decide to incorporate smartphone application technology into their mindfulness routine. When asked to define the meaning and purpose of mindfulness in their own words, 90% of the participants responded that mindfulness is about being aware of one's own body and thoughts. Half of these participants equated this awareness of the self in relation to their behavior, role, or perceived relationship with other people. This internal reflection is critical for the pursuit of mindfulness; these participants believe that at the core, mindfulness will help them to gain mental aptitude and acuity for their own wellbeing, while their ability to effectively engage with outside sources or build relationships with others is secondary in their goals for mindfulness.

Participant 2 reflects upon these benefits:

> [Mindfulness] is a better way to see the world…we are here together in the present moment, it is better for me to listen to you and give you my full attention. My interpersonal relationships are better, all the activities I do help me to enjoy [these relationships] and find value in them (Participant 2).

Every participant within this study each demonstrated a specific purpose for practicing mindfulness relating to their mental health. The overwhelming amount of coursework at UCLA and their stringent schedules were common reasons they provided for practicing mindfulness; they all were searching for some form of emotional and mental outlet that would allow them to regain mental clarity and peace of mind. Mindfulness, according to these study participants, is necessary for cultivating mental wellness by managing stress and anxiety associated with a busy and complex lifestyle, to help slow down and maintain control over their reactions to internal thoughts and external stimuli.

While stress and anxiety are the more common reasons for practicing mindfulness, several participants noted specific mental health issues in which they are actively working to manage. Participant 3 discussed her diagnosis of Obsessive Compulsive Disorder (OCD) and Trichotillomania, an impulse-control disorder that results in a repetitive behavior (“Trichotillomania (Hair Pulling),” 2013). For this patient specifically, this disorder manifests through repeated instances of hair pulling and skin picking behaviors. She exhibits behavior regulating actions to maintain control over these actions and to prevent them from consuming her thoughts and inhibiting her mental clarity. This participant learned through an associated study at UCLA that the best approach is to maintain a structured method of tracking symptoms and behaviors, increase awareness of this habit, and to actively pursue alternate behaviors to prevent these actions from occurring. Participant 3 focuses her thoughts to prevent these actions and embraces alternate behaviors, such as sitting on her hands when the desire to pick her skin is overwhelming. She also began to participate in yoga classes as an active means of regulating these behaviors, to "direct attention to something else and to fill [her] mind to replace bad or harmful behaviors with positive ones" (Participant 3). This participant practices mindfulness to keep her mind actively engaged. While she does not actively use mindfulness applications to track and regulate her symptoms, she is very interested in this idea and has downloaded several of these applications to explore to determine if they will be of benefit to her.

Participant 5 discussed the recent loss of an immediate family member and the associated mental and emotional repercussions of this event. Before it happened, she was primarily interested in enhancing and developing her wellness through physical fitness, however currently she is interested in finding ways to improve her mental health, both through destressing and managing her emotional state. For this participant, mindfulness is a mechanism for self-care in the event of loss or the imbalance in one's emotional state and to become attuned to mental health, in general. She also acknowledged the benefit that mindfulness might bring to her physical wellness as well, such that she might learn to direct her focus and engage certain body parts and muscle groups to enhance her fitness routine.

This emotional distress is also at the root of the mindfulness journey for Participant 10, who studied this practice spanning over the course of two decades. She began to learn about and study mindfulness resulting from many personal troubles that all occurred in a short period of time: she went through a messy divorce, her mother was diagnosed with cancer, two close family members passed away, and she struggled with unemployment. For Participant 10, mindfulness is a discipline that impacts her daily routine, from understanding her moods, controlling her physical health, regulating what she eats, and striving for self-actualization, by aiming to be happier and healthier emotionally while also becoming less judgmental and more compassionate towards others to better her personal and professional relationships. This participant chooses not to use mindfulness applications, due to her belief that true mindfulness is a personal routine that can only be established through mental aptitude and internalized self-discipline that cannot depend on an external regulation device.

Self-Regulation

As noted previously, the purpose of mindfulness is to become attuned to mental and emotional health by becoming more aware of internal responses to personal thoughts and moods, generally as a therapeutic technique. However, mindfulness is generally not biologically ingrained into one's psyche; like any skill to be mastered, practitioners of mindfulness must practice and routinely work to achieve this goal of mindfulness. Therefore, it is common for individuals to pursue ways that allow them to monitor and track their progress in pursuing mindful behaviors.

Each participant in this study appears to have an active thought processes when confronted about data collection practices in their preferred mindfulness applications. This thought process weighs a cost/benefit analysis to determine if the costs to privacy outweigh the personal benefits for using the application. Participant 6, who compared to other participants is more interested in the datafication elements of applications, said, “I’ve definitely always though ‘oh, I don’t need [those applications], but the curiosity of tracking my own progress is starting to overcome my previous, but still prevalent, concerns about privacy” (Participant 6). In general, as previously discussed, these applications propose great value to users who wish to help build habits and observe their progress over time. The data sharing industry that now regulates the application market forces users to make the choice between new and improved technologies to help better their mental and physical health or worry about the privacy of the data logged and tracked within these applications. Participant 8 consistently grapples with this question: “I am not sure of the long-term payoff. Does the benefit to my wellness outweigh the cost?” (Participant 8).

The participants in this study were all at various stages in their mindfulness journey; even Participant 10 who fully integrated mindfulness into her lifestyle continued to work on certain elements to better her life and to enhance her relationships with others. A common desire among the participants is to achieve mindfulness, but they are concerned that they do not have enough time to devote to this practice or that they are more willing to disregard mindfulness if they become too busy with other elements in their school or social lives. Participant 6 purported that physical activity and mindfulness is a commitment that can easily be negotiated due to school and work scheduling priorities. This practice, while perceived to be important for mental and physical health, must adhere to more time-consuming commitments. Participant 2, another active mindfulness practitioner, acknowledges that he is privileged to have enough flexibility in his schedule to devote to this practice.

He stated:

> I have a lot of time to do activities to cultivate mindfulness, free time that I can do those things, like I can take a lot of yoga classes or meditation classes and still have time to sit and meditate every day…a lot of people don't have the time and that is a lot harder… (Participant 2).

Time and commitment is a major factor in building habits and being persistent in maintaining these habits over the long term. Participant 3 reflected upon the difficulty of switching between not being mindful and being actively mindful; it is difficult to incorporate it at all times. Several participants also reflected upon the need for a timer as a reminder to take the time to meditate or track their mindfulness practice for that day. The participants also noted that smartphone applications allow them the ability to practice mindfulness outside the scope of a traditional Yoga or meditation class. Participant 8 stated that she wanted an application simply because it allowed her to manage stress or unwind after work if she was unable to attend Yoga class, "something I could do before bed, first thing in the morning, anywhere that didn't require me to change into workout clothes" (Participant 8). Applications allow for schedule flexibility, such that it is possible to meditate or engage with another mindfulness activity during a spare moment, rather than as an organized group activity that takes up a larger segment of their day. Mindfulness applications allow ease of use and simplicity for those seeking to monitor their behaviors during the process of habit formation. Mindfulness goals and specific use cases determine which applications are preferred. Participant 8 is very active with a busy schedule that does not allow much time for personal meditation sessions, although she does manage to attend a Yoga class multiple times in a week. She prefers to listen to guided meditations on her *Calm* application while she walks to work in the mornings. The app tracks which of the available preprogrammed meditations she chooses, typically based upon themes such as mood, stress, or anxiety, and how long she listens to the meditation. During our discussion, this participant was able to open her application to tell me how long her "streak" was for daily activity within the app—over one year.

Participant 7, on the other hand, is concerned about mindful eating; she wants to be aware of what she puts in her body every day. She keeps a consistent food journal through the application *Lifesum* which allows her to input every meal she eats. It also allows her to scan the barcodes of any food item to automatically log the information into her app, which promotes simplicity and accessibility such that she does not need to calculate nutrition information outside of the app for everything she eats. She has been very consistent with this practice; she has been using *Lifesum* daily for the last two years.

Participants 1 and 5 experimented with the application *Sleep Cycle* for some time. The purpose of this app is to track the amount of sleep the user gets every night and to wake them up with an alarm feature at the most efficient point in their sleep cycle the next morning. There are two ways the user's smartphone might track their quality of sleep: they can either place the device on their bed during the night, allowing the accelerometer in the device to track the sleeper's movements, or they can place the device on a bedside table allowing the microphone on the device to track sleep movements ("How it works," 2018). Neither Participant 1 nor Participant 5 found this application particularly useful for maintaining better sleep habits over a longer period of time, however they were more interested and curious about the graphs and charts that were created about their sleep patterns over a period of time, a reflection on the current trends toward datafication, the value found in the collective data, rather than in individual data points.

Application Datafication

One of the perceived benefits of using smartphone applications is the accumulation of tracked and logged data points that indicate trends and patterns in behavior over a certain period. Mindfulness applications, in addition to tradition wellness and fitness applications that track an individual's level of physical fitness, indicate the level of mindful activity in comparison to these levels previously. Participants 3, 8, and 9 use the *Weight Watchers* application to track their weight and fitness levels over time; Participant 9 has it connected to her Fitbit to track this progress. The applications allow users to monitor their behavior within the application to determine if they are on track for their goals within that certain area of mindfulness. 70% of the participants for this research project reflected positively on this element within the application, although Participant 1 noted that this element of tracking feels more intimate and personal, such that it records "a big sort of pattern in your lifestyle" (Participant 1). Datafication within applications is valuable to users because it offers personalized reports and recommendations based upon their previous activity. It reflects the shift in technology towards tools that can be integrated directly into an individual's social or personal life.   The level of personalization in these applications is intriguing to new users. Especially for those new to technology or to mindfulness applications specifically, they offer tools of analysis to help understand and interpret certain behaviors within their lives. Participant 6 is generally new to applications that allow her to track and monitor her physical and mental fitness levels. She is often introduced to these new applications by the students she works with at UCLA, one of which only recently informed her about the iOS Health application already installed on her iPhone that had been tracking her steps and location, charting how far she walks on any given day. Even though she generally is more conscious of her privacy through mobile devices, she values the information that iOS Health divulges about her life. She said:

> …that's really interesting because I never would have thought about how much walking I'm doing, what the stairs add up to…of course, it's like Pandora's Box where I want to find out more….[I have] a new sense of awareness about what [technology] is out there and how it can help me (Participant 6).

Participant 6's description of this event as Pandora's Box is reflective of her belief regarding the collection and datafication of her personal information; such like Pandora opening an intriguing jar and accidentally releasing the troubles of the world, she is concerned that she is inviting unwanted privacy and security violations by succumbing to her growing interest in these reports and charts about her activity.

Increased usage of these applications leads to the cumulation of more data points about the individual's usage habits. In this way, the application becomes more personalized to that individual. The patterns established through usage habits can be used to predict future user behavior and what content they prefer within the application. This personalization is especially important to Participant 8, who finds it valuable to know which meditations on the app *Calm* she listened to previously and which ones she liked. She wants the app to collect this information to generate new content based upon the ones that she likes. In this way, the increased personalization through the tracking and analysis of her data is beneficial to users, even though this might mean that *Calm* knows she is more interested in learning to regulate her emotional health than her level of stress management—elements that may be determined though her collected usage data.

RQ2: In What Ways are Mindfulness Practitioners Aware of Data Collection Practices in these Applications?

The level of understanding of data collection practices within mindfulness applications is reliant upon the awareness that users have about these practices in the first place. This awareness may be derived from their understandings generally of how data is generated collectively across various modes of technology, their perceived understandings of the role that targeted advertising plays in their lives, or popular presumptions derived from communication with others within their community who also use this form of technology.

Privacy Policies

The discussion of privacy policies with participants in this research study often began with slight embarrassment from the participant while I ensured them that I was not there to chastise them for their apathy toward privacy policies. Of all the participants interviewed in this study, only Participant 8 stated that she sometimes attempts to read a privacy policy, but not in-depth and not without uncertainty in her understanding of what the policy entails. According to this participant, she states, “Even if I read the privacy policies, I don’t feel like I totally understand the legalities…” (Participant 8). Participant 5 would agree with this assessment, as she noted that even if she did read the privacy policies, it would take her too long to decode the legal jargon that she believes is found within these policies.

Participant 3 shared her frustration with the privacy policy:

> I don’t ever read privacy policies, I don’t have time or care to read ten pages of the policy…I also heard that there are companies out there that expect you to not read them, that even if you click accept, they understand that you haven’t read it, and they understand that you aren’t really agreeing to terms, you just accept without reading…I am sure they are using my data or information but I don’t know if it’s being sold or something. But, if that was the case and I knew about it, I would choose not to subscribe to those apps at least, but are they all doing that?...it’s not like when you sign up, a thing pops up that tells you what information will be shared (Participant 3).

This uncertainty over the information reflected within the privacy policy was prevalent across the board for the participants in this research study. There appears to be a lack of understanding for the specific ways in which their data is used, despite the nature of the information collected within mindfulness applications.

Accessibility of the Policy

When discussing the role of privacy policies in the level of awareness people have regarding the collection and sharing practices of personal data within a smartphone application, it is important to discover whether the user would know how to find the privacy policy from within the application. Participant 2, after stating that he never saw the privacy policy and did not know that there was one, said that he did not know where to find the privacy policy because the settings on his preferred meditation application are very basic and limited. Participant 5 and 9, also when asked if they knew where to go to find the information in the privacy policy, stated they would either do a Google search, find the company website, or look in the settings on the application.

While there is general uncertainty of where one might go to find this policy, it should also be noted that these participants believe that in order to find this information, they need to search outside of their application.

One element that I discovered through this research study was the behavior of these participants relating to the trial and subsequent deletion of applications that they were no longer interested in. Participant 1, as noted previously with the discussion of the *Sleep Cycle* application, chose to delete this application because he did not find that it helped to improve his sleep and because he was uncertain if it was also tracking the sleeping behaviors of his roommate through the tracker in his microphone. He believed this to be too intimate regarding his personal behavioral patterns and was concerned about collecting information about his roommate without his consent. Participant 5 also demonstrated a trial period with applications, including *MyFitnessPal* and *Sleep Timer*, however she did not find it useful to log her calorie intake or track her sleep schedule through these applications, so deleted both. She also tends to download and test fitness applications to see if they work for her; for example, she tested the *Couch to 5K* application, decided she did not like that application, and deleted it. She addresses her process of determining which applications work best for her by stating that she goes "in and out of using apps" (Participant 5). Participant 7, similarly, tested "quite a few" food loggers, before settling on *Lifesum*, which she used for the last two years.

Application Permissions

Even though this research determined that, for the most part, these participants do not read privacy policies, they are must more active in controlling the tracking mechanisms in the applications that they download. Participants 5, 7, and 8 discussed these permissions: they all stated that they generally turn off Location Services and GPS permissions on their device for applications that generally do not need this information for its functionality. Participant 7 informed me of the ability to alter the settings on iOS applications to only allow Location Services when the application is in use. This action represents the interest in having control over specific types of data collection within applications. The participants of this study often refer to these permissions when discussing privacy and the various ways they attempt to retain control over the information that companies collect about them. The ability to turn off permissions or to deny the application access to various elements of the device demonstrates a sense of awareness over the ways application software might access personal information, but their understanding of how to resist this access is limited and may lead to a false sense of privacy security when using the application.

RQ3: What Influences the Levels of Concern that Mindfulness Practitioners Have about Data Security and Privacy of Data Collected and Shared by Corporations and their Affiliates?

Awareness of data collection practices in smartphone applications does not necessarily equate to a concern about these practices. There are various factors that may influence the level of concern demonstrated by the participants in this research study: trust in the company that distributes the application, a Cost/Benefit Analysis of the perceived benefits of using the apps in comparison to the cost to privacy and information security, and the level of resignation that these participants have in the data sharing industry as a whole.

Trust in the Application

The amount of trust that users have in an application is dependent on a number of factors: the amount of established trust in the company that created the application and the trust found in the social circles who recommend the application, whether this through friends and family or through social media by popular and well-received "Social Media Influencers".

The trust in the company itself depends on the level of perceived knowledge already established about the company. A consumer may be more willing to download a fitness application created by Nike than by another unknown company created primarily for the distribution of the application. The knowledge of this company and their products may increase the likelihood of discovery of the application. Participant 4, for example, prefers the Gaia Yoga a Meditation application because she is familiar with the brand and has purchased equipment from them previously. She stated, "Knowing it is from what I consider to be a reputable brand…it is an established company and not just some random yoga app that I don't know where it comes from, not that that should make me feel better, because I'm aware companies don't care about things like that…" (Participant 4). The user maintains this trust in the company based upon a standing relationship or previous interactions with that company. Participant 6 joined Club Pilates, for which she downloaded an application that allows her to keep track of the classes she attends and to set physical fitness goals. Her active participation within the organization, as well as the convenience and simplicity of class organization that the application offered, led her to download the app and use it to schedule and manage her fitness progress.

That said, it appears that the participants in this study lose trust in the application if there appears to be a greater number of targeted advertisements within the application or if the company management is sold or absorbed into another company. When Under Armor purchased the application *MyFitnessPal*, Participant 8 became more concerned about her rights as a consumer, especially in regard to the purpose for why she downloaded the free application to begin with. After the application was sold, Participant 8 witnessed an increase in targeted advertising and product placement within the app, along with an increase in email spam that she needed to opt out of. This change led her to believe that the company was more invested in selling her products that she did not want or need, rather than help support her in her fitness and wellness journey.

In this study, I was interested in determining how these participants found mindfulness applications and the process that they have to determine when to download and use the application. I determined that these participants were more likely to download an application if it was recommended by a trusted source, including friends and family or through trusted sources through social media. Participant 8 decided to subscribe to the *Calm* application only after it was recommended by people in her social circles. She stated, "I liked [the app] and people I know liked it, so I [may have downloaded the application because] people I trusted also trusted the app…in that way, I was more likely to purchase a subscription" (Participant 8). Similarly, Participant 2 downloaded the application *Headspace* after it was recommended to him by some close friends, although he prefers not to use it as it requires the use of headphones, a factor he prefers not to include in his meditations. Participant 6 only recently began learning about what all the world of applications has to offer due to her increased interactions with students who use these applications. Her discussions with these students and their introduction to the various ways technology can enhance her workout experience greatly impacts her interest in applications for wellness and the datafication elements found within them. Participant 7 relies on finding useful applications and other tools through her account on the social media website *Pinterest*. She states, "I find out about most of my apps through *Pinterest*…I feel like [they] know a lot about me, they recommend me things that I really would like to go look at" (Participant 7). This reliance on social media, that has personalized features about her tastes and interests, influences her decision-making process about which apps she might download. In this way, her trust in ability of her preferred social media site to determine what she might be interested in outweighs the trust that she has in the company behind the application.

Social relationships may also influence the decision to download applications based upon shared information within these groups about the security and privacy of these applications. For example, Participant 10, who generally does not trust any application with her information, trusts the messaging application *Signal* with her information because it is praised in her community and social networks for being secure and encrypted, although she has not read the privacy policy to confirm these perceptions. Participant 10 is a political activist and relies on this company to be forward about their data collection policies to ensure that information about her activities does not go into the wrong hands.

Targeted Advertising

Participant 3 has greater concerns about these data sharing practices, primarily relating to the use of targeted advertising through applications relating to mental health and mindfulness. She fears that if she were to use applications for specific mental health issues, advertisements may begin to reflect that issue. She states, “[When I use] the meditation for anxiety and for sleep problems, will I start getting advertisements for antidepressants and sleep aids? I am looking for alternative medicine for a reason” Participant 3). This question reflects a major concern among privacy advocates. Targeted advertising, which is inherently connected to the increased personalization trends among free apps, will lead to the monetization of mental health for these specific mindfulness applications. An individual’s personal concerns that they actively seek to remedy shifts from a private burden to a publicly accessible point of revenue. The cost of targeted advertising becomes another area to consider for consumers when pursuing a cost/benefit analysis for the usage of these applications.

Participant 3 enhances her argument against targeted advertising with a critique of these data sharing practices of her sensitive information to third-party advertisers:

> If I went to a psychologist or a therapist because I wanted counseling, there is an understanding that they aren't going to share my information, my information will be secure, it's private, and nobody will have access to this information except for me and the people that I approve. The same thing with the doctor, who has all of my information. Basically, these apps are like mental health and [physical] health apps, but they don't give you the same privacy that you would get at the doctor or at a psychologist's office. I think if they offer this service, they should make sure this information is secure, because this is my health information in the hands of somebody who obviously wants to harm me or get money out of me. The doctors aren't going to sell my health records to someone who wants to get money out of me (Participant 3).

This statement represents the inherent problem with the sharing and selling of sensitive data collected by these specific applications.

Anonymity

One of the most important factors that influence the cost/benefit analysis for the participants in this study is the level of anonymity given to their personal information. Some of the participants, including Participant 1 and 5, recognize that their information is beneficial to the company for statistical analysis for the application itself. They know that this information will help the application developers determine any flaws in the app and will use this collected information to improve upon it for later updates. Participant 2 also reflects on the app monetization process when they are free to download. He says that in order to deliver apps for free, a level of data sharing and selling must take place, however he wants the information collected about him to be anonymous—the developer must remove any personally identifiable information, including location data, from the source. Participant 5 and 7 agree with this statement, specifically as an element of personal safety. Participant 5 says that she is fairly open to the concept of sharing her data "as long as it won't potentially impact my safety, so maybe if my GPS was recorded, I would prefer that it wouldn't be shared liberally or at least without taking to me first" (Participant 5). Participant 7 says that she would delete the application in the event that she ever felt unsafe, however she did not indicate any plans to remove the collected data from the application servers. Participant 9 reflects upon her preference for anonymity. She states,

> I don't know if I've really thought about [privacy protection policies]. I guess it doesn't really matter that much to me, I just don't want my information shared publicly or linked to me…I don't really care what they do on the backend with that unless it gets linked to me or if it is not obscured in some way… (Participant 9).

Participant 9 prefers to use *YouTube* as her source for mindfulness and meditation due to the personalized connection she feels with content creators. When I asked her to compare the level of sensitivity between her *Weight Watchers* and *YouTube* applications, she stated, "they are about even because I don't want my weight to be public, but I definitely don't want my *YouTube* watch history to be public either. I would definitely want privacy around that, or at least anonymity" (Participant 9). While the preference towards anonymity is resounding among these participants, it begs the question of how anonymous they really are in the data collected and shared about them. For example, if they choose to login to these applications using their

Facebook or Google accounts, their behavior within these applications is more likely to be connected back to their personal accounts. While the drive towards anonymity is reflective of user preferences, it is important to understand how the increased connectivity of networked devices and accounts might influence this. The prevalence of interconnectivity though the trend towards Big Data may have a dramatic impact on the level of anonymity users might be able to achieve in their online activity.

Level of Resignation

When discussing their level of concerns with data collection practices in mindfulness applications, 80% of the participants indicated that they were resigned to these policies and the state of privacy in the current American economy. Participant 3 states,

> I don't know if there is anything that can be done because that's the world we live in. I know if we all just paid a dollar for these apps, then they won't have to sell our information, but at the same time, even if I paid for the premium *MyFitnessPal*, my information would still be stored there and would still have been stolen [in the 2018 data breach] (Participant 3).

Participant 4 shares this sentiment: "I assume everything I do, data is being gathered on me" (Participant 4). Participants 8 and 9 have reconciled the fact that this form of data collection is now prevalent in the world and is not what is necessary in order to live with technology. Participant 6 expands on the same worries about the state of this data sharing economy, pensive about the normalization of this act across generations over time.

She states,

> I'm sure there are a lot of people out there who don't think about this and I think that's going to be increasingly worse…it might be that your information is already out there, who cares, might as well get some benefits from it. Especially with newer generations, everything is turning to technology. I feel like it will become a lot more acceptable (Participant 6).

The participants in this study grapple with the desire to use this technology to better their mental and physical health, to develop patterns in their behavior and build routines around mindfulness and meditation, but at the cost of their personal information added to the ever-growing network of information about technology users. They recognize that in order to receive the benefits that these applications have to offer, it is necessary to submit to the data sharing practices of Big Data that govern this data-driven economy. Participant 10 reiterates the idea that this is only going to be more relevant with future generations: "Do you know the whole thing about the frog that is in the pot of water? If it was thrown into the pot, it would try to get away, but if you warm the water up slowly while it is in there, the frog gets cooked" (Participant 10).

DISCUSSION

The interviews with mindfulness practitioners reflect the range of beliefs and perceptions regarding data collection practices in mindfulness applications. Despite the limited number of participants in this study, they represent a large range of attitudes about these practices that I believe are reminiscent of the debate over privacy through applications. There are several important points about these attitudes that are determined by the research questions proposed in this study: the desire to pursue mental health and wellness, the ways in which application permissions might be the primary ways in which users understand how companies collect their data, the overarching trend towards datafication, the perception of anonymity through their collected data, and any folk presumptions I determined based upon the interviews in this study. Each of these elements direct the conversation about these perceptions of data collection and should be further researched in order to reflect upon how they dictate user understandings of data collection practices through applications, in general.

Promotion of Mental Health and Wellness

The mindfulness practitioners that I interviewed for this project were particularly interested in self-regulation to enhance their overall mental health, wellness, and interactions with their peers. They practice mindfulness to become aware of their thoughts and behaviors as indicative of their current mental state, resulting from depression, stress, or anxiety. Each of the practitioners I spoke with for this project believed that mindfulness is a valued practice that must be learned and practiced to find happiness and contentment in their lives.

The process of mindfulness as an approach to remedy mental health issues is a method substantiated by traditional cognitive-behavioral therapeutic approaches (Sipe & Eisendrath, 2012). For two of the participants in this study, certified therapists or psychologists directed them toward this method specifically as a therapeutic technique. These participants had problems with either depression and anxiety or other mental disorders including Trichotillomania. This promotion by experts in the field of mental health directed these participants to the practice of mindfulness and one of the ways in which mindfulness is accessible to the public is through smartphone applications. These applications offer tools that allow the average user with limited knowledge in cognitive-behavioral therapy and self-regulation to develop skills and build habits within these specific areas. As previously studied by Bandura, users are particularly interested in the concept of self-regulation, through logging and tracking, and self-diagnosis based upon this documentation (Bandura, 1991). This project represents a very specific area of self-regulation as it builds upon habit-building goal-oriented behaviors beyond physical fitness to the realm of mental wellness.

Permissions as the New Privacy Policy

The participants of this study, in general, are aware that there are data collection practices within mobile smartphone applications, however the extent to which they are aware of the privacy ramifications is dependent upon the type of mindfulness application they prefer. For example, they are more likely to be aware of the potential for data collection activities in more personalized applications, that require logging personal data into the application, although the level of awareness increases when this information relates to physical health, such as height and weight, compared to information about eating behavior, as an example.

This project demonstrated that the participants were far more familiar with data collection practices if they were referenced in the application permissions. Because these participants rarely read the privacy policy for the application, they were more reliant on the permissions to determine what the application requests access to, in comparison to other forms of data collection within the app. This finding correlates to the study produced by Reidenberg et al regarding the limited understanding and usage of privacy policies (2015). The participants were wary of the privacy policies in general and were more likely to ignore the document in their decision-making processes for which application best suits their needs. This finding is also substantiated by Steinfeild, who discovered that few users read the privacy policy overall, however if the policy was given to users by default, they are more likely to read the document (2016). The actions of the participants in my research study may also demonstrate the increased likelihood of understanding the permissions for the application, especially since it is not as complex as a privacy policy and it dictates to users exactly which parts of the user's smartphone it will have access to.

This might represent an element of control that users believe they have over the collection of their personal data. As determined in the findings of this research study, users are generally more concerned about the location-tracking capabilities of their devices for applications that do not explicitly need location for its functionality. The permissions inform the user if the application requests access to the device GPS or Location-Services. The participants of this study are less concerned about the location-tracking capabilities of their devices if they have the ability to disable Location Services while outside of the application. Privacy advocates and technologists debate the extent to which this function actually disables the application's ability to track the user's location, however; there are alternate ways beyond GPS to track a user's location, including the knowledge of an individual's starting point in conjunction with their device's accelerometer, the environment's air pressure, and elevation mapping (Mosenia, Dai, Mittal, & Jha, 2017). The process of viewing the application permissions and actively turning off Location-Services for a device decreases user concern about data privacy, due to the misunderstanding of the ways application designers might collect location information.

The Trend Towards Datafication

The participants in this research study who prefer to use mindfulness applications demonstrate interest in the datafication elements of applications that reflect their trends and patterns over time. This interest is derived from the desire to build habits and increase good behaviors related to mindfulness, meditation, and self-regulation. As confirmed by Li, Dey, and Forlizzi, this trend towards personal informatics allows users to take an active role in the collection and processing of their data relating to these behaviors. In general, the perceived benefits of datafication, for tracking and measuring these patterns, outweigh the cost to personal privacy, whether the participant felt great concern for privacy or not. For example, even though Participant 6 is already concerned about data collection practices and privacy in general, she was willing to forgo those hesitations in order to reap the benefits of tracking her fitness and meditation over time. In the same way, Participant 7 had little concern about data privacy but had similar interests in reflecting upon her eating habits over a period of time. It is important to note, however, that there may be a third variable to this trend towards datafication: those who are more active on their smartphones or technology in general may be more likely to use and perceive the benefits of these applications. Those who desire to incorporate technology into all parts of the social and personal world might already be primed to value these elements of datafication. This might also be enhanced by the amount of resignation felt toward privacy and data in the modern technological world. When the user perceives that there is nothing that can be done about these data collection practices, and that all of their online actions will transmit personal data of some form or another, they are more willing to reap the perceived benefits of datafication.

I believe this to be the core issue determined from this research project: mindfulness practitioners are very interested in the tracking and logging elements that are crucial for habit and routine building. They display the same goal-oriented behavior of an athlete tracking their speed or agility over time, or as a beginner gym member wanting to log their weight loss over time. There is an overarching trend in which smartphone users are looking to technology for the simplicity and ease of use in these tools that allow them to become, what they perceive to be, better versions of themselves in order to obtain happiness and self-worth. It is important to reflect upon the trade-off that users have when they begin to self-regulate through these applications; the way that it currently stands in the modern tech industry, individuals have to decide between modern tools for achieving personal goals and retaining control over their personal information.

The Preference for Personalization

The Personalization-Privacy Paradox was evident within this research study. The level of personalization agrees with the extent to which the user desires datafication elements in their applications, as I discussed in the last section. In agreement with the previous research of both Hann and van Dijck, the participants were more willing to forgo privacy concerns in order to receive the benefits presented through the datafication elements of their mindfulness application (Hann et al., 2002; van Dijck, 2014). The personalized elements of these applications, such as the logging and tracking features embedded within, enhance the overall experience of these applications for the user's benefit. As demonstrated through this research project, and in agreement with Liu et al, if the user perceives the application to be useful, such that it might boost their performance, they are more willing to forgo their privacy by imputing their personal information into the app (2014). However, users might be less inclined to share their information if they do not trust the organization to keep their information safe, as represented through the *MyFitnessPal* breach and the decreased usage of this application over time by these research participants as a result.

The Perception of Anonymity

This study found that mindfulness practitioners have a wide range of concern regarding data collection within their preferred applications, however generally, this concern is mitigated by the perception of anonymity within the data collected. When the user believed that their personal information was only collected in aggregate for purposes such as application management and statistical analysis, they were less concerned and more willing to share their data with these companies. These findings are consistent with the findings by Pedro et al and Gustarini et al (2016; 2013) . It is important to note that this perception of anonymity may not reflect accurate data collection practices within these applications. For example, while the application developer may use aggregate information about its users to promote the functionality of its application, the control over aggregate data is diminished when users log in to that application through an alternate API, such as though Facebook or Google. Similarly, there are discussions regarding the validity of anonymity through technology due to its increased interconnectivity with other services due to Big Data and collective Datafication. There is the argument that anonymity is easily diminished due to the likelihood of Reidentification resulting from the increased number of data points collected about each individual (Ohm, 2009). Also, the context around the usage of the application itself, beyond the collected data within the app, signifies great insight into the individual’s character and state of health. For example, while users may not be as concerned sharing their information about their habits when simply listening to a guided meditation through their application, the choice of which meditation they chose to listen to, such as one for depression or anxiety, details the individual’s mental state at that moment and over the course of the usage of the application. An employer or an insurance company might have greater interest in knowing that an employee actively engages with mindfulness or other health-based applications, as an indicator of either greater health concerns or increased interest in personal welfare, while the data itself might be secondary.

Folk Presumptions

Based upon the interviews in this research study, it appeared that there were several instances of what I have termed “folk presumptions” found within these discussions. Folk presumptions are popular understandings of how data sharing within mobile applications, generally passed through word of mouth, whether true or untrue. These understandings may be derived though mass media, communication between other users, or misinterpretations of privacy policies or data sharing practices in general.

Free, Paid, Subscription

As determined through the participants of this study, there is a perceived difference in the data collection practices of mobile applications for those that are ‘free’ initially, meaning that these applications are available for download without charge from the application store, and those that come with a pay wall, where a fee is paid at the time of download. This paid app structure is divided into two types of applications: a one-time fee at the time of initial download or a subscription model, in which the user repeatedly pays for the continued service of the application. There appears to be the persistent belief that applications are less likely to use an individual's personal data for sharing or selling to potential advertisers if they either pay for or subscribe to the application, as opposed to downloading the application for free. This perception is based upon generalized understandings of the ways in which applications monetize their product, however this is not based upon specifics of the application's practices, as determined through the company's privacy policy.

Participant 8 pays for a subscription to the guided meditation application *Calm*. She states, "I don't know if this is true, but I feel like there is some form of responsibility and trust [by the company]…there is a more reasonable expectation that they would be more up-front with your data when you pay into the apps" (Participant 8).

She later adds,

> If [paying for an app] helps make the company better, make better content, and if it helps them not have to sell my data to fund themselves for free…I think that is a larger extent of what is happening, because they don't charge a fee, they have to sell your data…that is why I trust the paid apps more because their funding model might be a little more stable. Maybe not as much as I want to be, but I don't think I've ever been pushed an ad in *Calm* (Participant 8).

Similarly, when Participant 9 was questioned about who she believes already has access to her information stored in *Weight Watchers*, she states,

> I have no idea what they do with that information. I assume they aren't dependent on your data because you pay for the app, and pay for the service, so I wouldn't be as concerned with them using my data, because they really don't need to (Participant 9).

These preconceived notions need to be examined in further depth. The assumptions about data collection models may dramatically affect the relationship between app developers and consumers in building trust between them, however this may also have a larger impact on user protections over their personal data. It is important to be critical of this belief as it is yet to be determined if there is truth found in this folk presumption.

Privacy Policies are for Social Media

This lack of understanding of privacy policies, as demonstrated previously in this paper, is enhanced through Participants 7 and 9, who appeared to believe that the privacy policy was intended primarily for security features for the application or the social media elements found within it. When I asked Participant 7 how the privacy policy impacted her decision to download *Lifesum,* her meal tracking application, she stated,

> I think with *Lifesum* there is a social media aspect, but I don't use that…I want to keep the information to myself, keep it private, I don't think I looked at the privacy policy in-depth because I used this one email I use for all [these applications] so I don't really care if that email gets hacked…I did not look at the privacy policy in-depth, just accepted the terms and conditions (Participant 7).

This misconception may be derived from the colloquial discussion of privacy policies and the ways in which people might disregard the terms and conditions, as promoted through popular culture and social media. Similarly, the discussion of privacy and data within applications is typically connected to discussions of information security, therefore it may easily be presumed by those not actively engaged in tech circles that privacy and security are interchangeable. Participant 9, in addition to also correlating the privacy policy with social media, suggested that her *Weight Watchers* app was "self-contained"; while this may be a comment reflecting on the social media aspect to this app, in which users might post and share any updates in their weight loss journey, this may be an indication of a preconceived notion that only she might have access to that information, contained within the application on her phone without any access from others externally, in the same way that one might only have access to notes written in a paper journal. This element is crucial in understanding user perceptions and awareness of data collection practices in applications and should be further assessed in future research.

Trial and Deletion

Many participants of this study discussed their process of determining which applications best suit their needs; they often download the application and sign up for an account—when necessary— before testing the application and deleting it if it does not meet their expectations. There is an inherent problem with this 'trial and deletion' phenomenon that occurs when deciding upon which application is best for the individual's purposes. For most of these applications, it is necessary to either make an account with that company or log-in with Facebook or Gmail to access the application interface. This means, that even though an individual may only use the application for a short period of time before making the decision to no longer continue, the account with their information will remain under their name. The deletion of these applications typically refers to the deletion of the application from the smartphone, but users are much less likely to contact the company to remove their information from their servers after this deletion.

Participant 8's experience with *MyFitnessPal* exemplifies this issue: she used this application for quite a while but decided to cease usage of this app due her decreased desire to actively log her calorie intake. She stopped using the application, however was later informed about the *MyFitnessPal* security breach in March 2018. She was less concerned about this breach as she never entered credit card information into the app, however she is concerned about her information that was stored on the MyFitnessPal servers. This problem begs the question of how many applications users might ‘trial and delete’ and if there are any overarching concerns with the account information and privacy attributed to these applications.

Institutional Concerns

The question of privacy concerns over the data collected by mindfulness applications extends beyond individual choices and personal responsibility. Through this study, I interviewed UCLA students who participate in campus mindfulness-related activities that are endorsed by the university. The university invests in mindfulness-related activities that promote wellness for its students and develops programs that help students build better habits and to achieve goals related to physical, mental, and emotional health. The university endorsement of mindfulness is not inherently negative or harmful and may be an act of good faith by an educational institution. However, this begs the question of the responsibility that the university has over the way students, faculty, and staff incorporate data-harvesting applications into their mindfulness routines. If the university advocates for the usage of a mindfulness application to promote mental health—and that application collects and shares a student’s personal and private information as denoted through the application privacy policy—should the university be held accountable for ensuring the student is informed of these practices? University officials need to understand and depict the implications of the usage of these mindfulness applications and the resulting damage to that user’s privacy. The university should also educate students, in general, of data collection and sharing through smartphone applications and promote best practices to teach students the steps they can take to enhance their personal privacy while using these applications. The university's goal should be to prioritize student awareness and understanding of data collection practices to inform and educate students about an issue that fundamentally affects their identity in a digital world.

CONCLUSION

Mindfulness applications reflect a fundamental flaw of Big Data, mass consumerism, and the modern surveillance state. In today's world, technologists, social media influencers, doctors and therapists, and friends and family all claim that the best way for an individual to take control of their life, body, and mind is to incorporate gadgets and technology into their daily routine. These technologies allow users to track and log their behaviors, reflecting upon their overall health and wellness—physically, mentally, and emotionally. These applications reflect the culture of surveillance capitalism, as depicted by Shoshana Zuboff, through the ways that mobile applications encourage "the migration of everydayness as a commercialization strategy" (Zuboff, 2015, 76). Companies now rely on the personal and private information that they collect from their userbase as the primary way to earn a profit, eradicating elements of democracy and consumer choice through this act. These companies generate "hyperscale assemblages of objective and subjective data about individuals and their habitats for the purposes of knowing, controlling, and modifying behavior to produce new varieties of commodification, monetization, and control" (85). By making mindfulness a commodity, it forces users to choose between modern tools for self-improvement and their digital privacy—which may not even be a choice at all as users tend to rationalize this exchange through resignation of modern data collection practices— to create a new marketplace based primarily on user health and behavior. This market might later have genuine consequences if other companies that have a stake in our welfare have access or control over this information, including insurance companies, health care providers, or employers. This study demonstrates the negative impact of surveillance capitalism on consumer welfare and the ways that it might subjugate those that incorporate these applications into their mindfulness routine.

I advocate for a reevaluation of the pay structure within these applications as they have the ability to produce more harm to personal welfare than good simply for companies to earn a profit. As with all other products available for purchase online, application users should be willing and able to pay an initial fee set at a competitive market price for the services they value. Those that value mindfulness and want to learn how to be more mindful through an application should be willing to pay for these services. Big data is actively shaping our society and it is necessary to understand the overarching impact of this if Americans want to retain control of their data and how they want the future of our nation to unfold. We need to think radically about these business models where there is extremely sensitive information about what makes us human that is now subject to becoming a commodity for big business. As Dr. Veronica Barassi stated, this is not solely a concern about consumer and consumer rights, it is about citizen and citizen rights (2018).

APPENDIX A: INTERVIEW QUESTIONS

INTRODUCTION

The purpose of this interview is to discuss mindfulness, smartphone applications, and privacy. The interview will last about 30 minutes. Please review and sign the attached Informed Consent form and direct any questions to the Primary Researcher. The researcher will begin recording audio after the participant signs all necessary documentation.

1. What does the word ‘mindfulness’ mean to you?
    a. What value do you find from practicing mindfulness?
    b. Are there any areas of your life that it helps to enhance or make better?
    c. Are there any problems or difficulties with practicing mindfulness?
2. Please describe the current ways you practice mindfulness.
    a. Please illustrate your mindfulness routine and any specific activities that you do.
    b. For how long have you practiced mindfulness? How often?
    c. For how long in one sitting?
3. How do you incorporate technology, such as smartphone applications, into your mindfulness routine?
    a. What specific smartphone applications do you use?
    b. How did you choose them?
    c. How often do you use mindfulness applications? In what ways do they supplement your tech-free routine?
4. How did the privacy policies influence your choice of application?
    a. How easy or difficult is it to find information about the company’s data collection practices on the privacy policy?
    b. What kind of privacy protections would you like to see represented in these policies?
5. What kind of information would you be comfortable revealing in these applications?
    a. How would you describe the level of sensitivity of your information in this application?
6. Who would you be willing to share the information in your apps with?
    a. Who do you think should have access to this information?
    b. Who do you think already does have access to this information?
7. Please describe your overall relationship with your mobile phone and applications.
    a. In what ways do you primarily use your phone?
    b. Is it primarily a tool for work/business or do you use it for play/fun?
    c. Do you download apps often? Free or paid?

REFERENCES

Am I Hungry? Mindful Eating Virtual Coach App - Am I Hungry? (2018). Retrieved May 16, 2018, from https://amihungry.com/marketplace/mindful-eating-virtual-coach-app/

Bandura, A. (1991). Social Cognitive Theory of Self-Regulation. Organizational Behavior and Human Decision Processes, 50, 248–287.

Barassi, V. (2018, May). Child | Data | Citizen: Datafication, Algorithmic Inaccuracies, and the Profiling of Future Citizens. Presented at the Reclaiming Expertise Conference, University of California, Los Angeles.

Davis, D. M., & Hayes, J. A. (2011). What are the benefits of mindfulness? A practice review of psychotherapy-related research. Psychotherapy, 48(2), 198–208. https://doi.org/10.1037/a0022062

Federal Trade Commission. (2016). Big Data: A tool for inclusion or exclusion? Understanding the issues (FTC Report). Retrieved from https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf

Federal Trade Commission Act. (2013, July 19). Retrieved December 15, 2017, from https://www.ftc.gov/enforcement/statutes/federal-trade-commission-act

Friese, M., & Hofmann, W. (2016). State mindfulness, self-regulation, and emotional experience in everyday life. Motivation Science; Washington, 2(1), 1–14. http://dx.doi.org/10.1037/mot0000027

Glenn, T., & Monteith, S. (2014). Privacy in the digital world: medical and health data outside of HIPAA protections. Current Psychiatry Reports, 16(11), 494. https://doi.org/10.1007/s11920-014-0494-4

Global big data industry market size 2011-2027 | Statistic. (2018). Retrieved May 22, 2018, from https://www.statista.com/statistics/254266/global-big-data-market-forecast/

Grossman, P., Niemann, L., Schmidt, S., & Walach, H. (2004). Mindfulness-based stress reduction and health benefits. Journal of Psychosomatic Research, 57(1), 35–43. https://doi.org/10.1016/S0022-3999(03)00573-7

Gustarini, M., Wac, K., & Dey, A. K. (2016). Anonymous smartphone data collection: factors influencing the users' acceptance in mobile crowd sensing. Personal and Ubiquitous Computing, 20(1), 65–82. https://doi.org/10.1007/s00779-015-0898-0

Hann, I.-H., Hui, K.-L., Lee, T., & Png, I. (2002). Online Information Privacy: Measuring the Cost-Benefit Trade-Off. ICIS 2002 Proceedings. Retrieved from http://aisel.aisnet.org/icis2002/1

Harris, K. (2014). Making your Privacy Practices Public, 28.

Health App Use Scenarios & HIPAA. (2016). Retrieved from https://hipaaqsportal.hhs.gov/community-library/accounts/92/925889/Public/OCR-health-app-developer-scenarios-2-2016.pdf

Herrmann, M., Hildebrandt, M., Tielemans, L., & Diaz, C. (2016). Privacy in location-based services: An interdisciplinary approach. SCRIPTed: Journal of Law, Technology and Society, 13(2), 144–171.

Hill, K. (n.d.). How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did. Retrieved May 16, 2018, from https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/

HIPAA Privacy Rule and Sharing Information Related to Mental Health. (2017), 13.

How it works. (2018). Retrieved May 12, 2018, from https://www.sleepcycle.com/how-it-works/

Khoury, B., Sharma, M., Rush, S. E., & Fournier, C. (2015). Mindfulness-based stress reduction for healthy individuals: A meta-analysis. Journal of Psychosomatic Research, 78(6), 519–528. https://doi.org/10.1016/j.jpsychores.2015.03.009

Li, I., Dey, A., & Forlizzi, J. (2010). A stage-based model of personal informatics systems, 10.

Liu, Y., & Simpson, A. (2016). Privacy-preserving targeted mobile advertising: requirements, design and a prototype implementation. Software: Practice and Experience, 46(12), 1657–1684. https://doi.org/10.1002/spe.2403

Liu, Z., Shan, J., Bonazzi, R., & Pigneur, Y. (2014). Privacy as a Tradeoff: Introducing the Notion of Privacy Calculus for Context-Aware Mobile Applications. In 2014 47th Hawaii International Conference on System Sciences (pp. 1063–1072). https://doi.org/10.1109/HICSS.2014.138

Mayer, J. R., & Mitchell, J. C. (2012). Third-Party Web Tracking: Policy and Technology (pp. 413–427). IEEE. https://doi.org/10.1109/SP.2012.47

Mobile Health App Developers: FTC Best Practices. (2016, April 4). Retrieved May 14, 2018, from https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-app-developers-ftc-best-practices

Mobile Health Apps Interactive Tool. (2016, April 4). Retrieved December 14, 2017, from https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool

Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff. (2015). Retrieved from https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf

Mosenia, A., Dai, X., Mittal, P., & Jha, N. (2017). PinMe: Tracking a Smartphone User around the World. IEEE Transactions on Multi-Scale Computing Systems, 1–1. https://doi.org/10.1109/TMSCS.2017.2751462

Reidenberg, J. (2015). Disagreeable privacy policies: mismatches between meaning and users' understanding. Berkeley Technology Law Journal, 30(1), 39.

Ruckenstein, M., & Schüll, N. D. (2017). The Datafication of Health. Annual Review of Anthropology, 46(1), 261–278. https://doi.org/10.1146/annurev-anthro-102116-041244

Shea, C. (2018). A Brief History of Mindfulness in the USA and Its Impact on Our Lives | Psych Central. Retrieved May 16, 2018, from https://psychcentral.com/lib/a-brief-history-of-mindfulness-in-the-usa-and-its-impact-on-our-lives/

Shilton, K., & Greene, D. (2017). Linking Platforms, Practices, and Developer Ethics: Levers for Privacy Discourse in Mobile Application Development. Journal of Business Ethics, 1–16. https://doi.org/10.1007/s10551-017-3504-8

Sipe, W. E. B., & Eisendrath, S. J. (2012). Mindfulness-based cognitive therapy: theory and practice. Canadian Journal of Psychiatry. Revue Canadienne De Psychiatrie, 57(2), 63–69. https://doi.org/10.1177/070674371205700202

Steinfeld, N. (2016). "I agree to the terms and conditions": (How) do users read privacy policies online? An eye-tracking experiment. Computers in Human Behavior, 55, 992–1000. https://doi.org/10.1016/j.chb.2015.09.038

Sutanto, J., Palme, E., Chuan-Hoo Tan, & Chee Wei Phang. (2013). Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users. MIS Quarterly, 37(4), 1141-A5.

The world's most valuable resource is no longer oil, but data. (2017, May 6). The Economist. Retrieved from https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource

Trichotillomania (Hair Pulling). (2013, October 14). Retrieved May 12, 2018, from http://www.mentalhealthamerica.net/conditions/trichotillomania-hair-pulling

Tsavli, M., Efraimidis, P. S., Katos, V., & Mitrou, L. (2015). Reengineering the user: privacy concerns about personal data on smartphones. Information and Computer Security, 23(4), 394–405. https://doi.org/10.1108/ICS-10-2014-0071

Tucker, P. (2013). Has Big Data Made Anonymity Impossible? MIT Technology Review, 116(4), 64–66.

UCLA Recreation - FITWELL. (2018). Retrieved May 7, 2018, from http://www.recreation.ucla.edu/fitwell

Van Dam, N. T., van Vugt, M. K., Vago, D. R., Schmalzl, L., Saron, C. D., Olendzki, A., … Meyer, D. E. (2018). Mind the Hype: A Critical Evaluation and Prescriptive Agenda for Research on Mindfulness and Meditation. Perspectives on Psychological Science, 13(1), 36–61. https://doi.org/10.1177/1745691617709589

van Dijck, J. (2014). View of Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. Surveillance & Society, 12(2), 198.

Werner, M. (2016). Privacy-protected communication for location-based services. Security and Communication Networks, 9(2), 130–138. https://doi.org/10.1002/sec.330

Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. Journal of Information Technology, 30, 75–89.