EMPLOYING RESEARCH-BACKED TECHNIQUES TO DECREASE ATTRITION IN MINDTRAILS PROJECT

DISCUSSING CURRENT AND FUTURE U.S. LEGISLATION REGARDING DATA PRIVACY

A Thesis Prospectus
In STS 4500
Presented to
The Faculty of the
School of Engineering and Applied Science
University of Virginia
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Systems Engineering and Environment

By
Darby Anderson

October 31, 2019

Technical Project Team Members
Amanda Brownlee, Camryn Burley,
Georgie Lafer, Taylor Luong, Meaghan McGowan,
Judy Nguyen, William Trotter, Halle Wine

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Signed: Darby Anderson Date: 10/31/2019

Approved: Catherine D. Baritaud Date: Dec. 5 '19
Catherine D. Baritaud, STS Division, Department of Engineering and Society

Approved: Laura Barnes Date: 11/6/19
Professor Laura Barnes, Department of Systems Engineering and Environment

Whether from too much screen time, not enough social interaction, or unrealistic physical standards, people in the U.S. are suffering from anxiety and mental health problems. This past year, roughly 50 million people were diagnosed with some form of mental illness, but less than half received treatment for it (National Alliance on Mental Illness [NAMI], 2019, p. 1). Stigma surrounding seeking treatment may contribute to this disparity as well as a lack of professional help, high cost of service, poor insurance coverage, lack of desire, and mistrust of psychologists and other mental health professionals (Harvey & Gumport, 2015). Trends toward mobile and electronic intervention have exposed more individuals to treatment, however these online programs fail to retain users for the entire duration of the course. The concept of mobile health (mHealth) and electronic health (eHealth) intervention has been accepted by mental health professionals, but many apps and online programs do not employ research-backed techniques (Price et al., 2013). This same study also found major privacy and security issues concerning personal data with mHealth intervention.

The technical and STS research will explore these two potential failures of eHealth and mHealth. The technical team will research evidenced-based practices to include in an online anxiety reducing program. Collaborating with Psychology graduate students, we will employ proven techniques that individuals can rely upon to improve their mindset and mental health. During the implementation process, we will also consider ways to safeguard participants' information in the case of a privacy breach or stolen computer. Tightly coupled with this extension, the STS research focuses on how the Health Insurance Portability and Accountability Act (HIPAA) can be updated to reflect new technology and other foreign legislations. It will investigate ways to further protect personal health information (PHI) through both the use of further encryption standards as well as additional disclosure and transparency regulations.

MINDTRAILS: A CALM THINKING PROJECT

Under the guidance of Engineering Systems and Environment Professor Laura Barnes and PhD candidates Anna Baglione, Jeremy Eberle, and Alana Parsons, Systems Engineers Amanda Brownlee, Camryn Burley, Georgie Lafer, Taylor Luong, Meaghan McGowan, Judy Nguyen, William Trotter, Halle Wine, and I will investigate ways to decrease attrition and increase the quality of the MindTrails online program. One third of the population is affected by an anxiety disorder without any signs of prevalence dropping (Bandelow, B., & Michaelis, S., 2015). Funded by the National Institutes of Health (NIH), the MindTrails Calm Thinking study hopes to reduce this number by using cognitive bias modification targeting interpretation (CBM-I) techniques to change the mindset of the highly anxious individual. Implementation of CBM-I includes scenarios that convey a neutral or negative situation including a reaction statement with missing letters for the participant to complete (MacLeod, 2012). Repetitive tasks that involve reading scenarios and completing positive reactions have succeeded in reducing anxiety for highly anxious individuals (Steinman S.A. & Teachman B.A., 2010). However, despite incorporation of this successful technique in the MindTrails online program, attrition rates have increased. Last year's capstone team determined that adding implementation intentions and personalization to the scenarios would help with increasing retention and the satisfaction of participants (Azevedo et al., 2019).

Implementations intentions involve setting a goal that is specific enough to answer the questions when, where, and how. The combination of forming a goal and a reaction causes this technique to be more effective than goal-setting in general (Webb, T.L., Ononaiye, M.S.P., Sheeran,P., Reidy, J.G., & Lavda, A., 2010). A study conducted by Webb et al. in 2010 found that highly anxious individuals performed equally as well given a task after receiving a set of

implementation intentions compared to not anxious individuals. Since CMB-I focuses on reshaping the way anxious individuals respond to embarrassing or negative situations, implementation intentions couple well with this psychological strategy by creating a specific goal. Figure 1 illustrates the coupling of the two techniques regarding an overarching goal chosen by the MindTrails participant. The first box would have been one chosen from multiple goals to achieve with the program. After selecting a goal, the user would be given situations that they would have to respond to via a multiple-choice answer. The example illustrated two people laughing, which could be misinterpreted as two individuals laughing at the participant. However, CBM-I attempts to change the way the individual thinks by letting them complete the reaction to the scenario. The reaction is "This means they are f_n"; the user then has to pick from a combination of letters completing the sentence. The correct answer would be "u" and would allow the individual to consider for at least a moment the better way to respond to a neutral or possibly negative situation in their eyes. Additionally, including an implementation intention to the scenario would also develop a related goal that the person can later use in real life.

Figure 1: CBM-I and Implementation Intentions: Combining the effects of changing someone's attitude towards anxious events and setting specific goals will improve participant's thought process and behaviors. (Anderson, 2019).

The example explained above also incorporates the concept of personalization by allowing the user to select the goal he or she wishes to achieve. This feature can extend even more however with specific situations concerning the participant's demographics. An app that currently reflects an extremely personalized mHealth intervention is called the Challenger App. It aims at reducing social anxiety via personalization and gamification techniques. Designers

focused specifically on personalization by giving the users the ability to send feedback on certain challenges and situations deemed too difficult, easy, or unrelatable (Miloff, A., Marklund, A., Carlbring, P., 2015). Since most apps available do not incorporate personalization and gamification techniques to this degree, the Challenger App will be used as a guideline in developing similar strategies with MindTrails.

The capstone team will address the attrition problem by splitting into two subgroups; one subgroup will focus on incorporating personalization in scenarios, while the other will develop more on implementation intentions and goal setting. Extensive literature review on these two techniques will be done in advance of wireframing and coding. Since MindTrails involves mental health issues with highly anxious individuals, it is imperative that proper studies and research support methodologies and framework. Working with Psychology graduate students and Computer Science undergraduate students will help gain perspective from multiple backgrounds and viewpoints. The Psychology graduate students will be in charge of developing the personalized scenarios and implementation intentions while the Systems undergraduates manage the transition from idea to construction. Computer Science students will code the final product into a mobile app and online program.

Since research and project management will be the main focus for the Systems capstone team, additional resources are not needed. Access to codes and programs through GitHub will allow team members to manipulate or revise code if needed. Figma will be used for wireframing design ideas for the website and app to serve as guidelines for the Computer Science students. Communication between the Psychology students and Computer Science students will be the main focus for the team members as well as ensuring that requirements from the MindTrails leaders Laura Barnes and Bethany Teachman are met.

After the completion of the year-long project, we hope to deliver an improved online program and the beginning stages of the MindTrails app. Before we can do so, proper research and planning must be made during the first semester. All wireframes and literature reviews will be completed by December. Furthermore, tutorials on the coding language used for the website and mobile app will be completed by December in order to begin timely developments for code creation. By February, code should be finished to render the wireframes created in the previous semester. Code reuse should be available to develop similar components in the app, so a deadline of March requires the app reflect similar changes in the website. During the month of April, transitions should be made to pass on codes and wireframes to the MindTrails team. A paper detailing the process code rendering and application is due by May, thus all work should be completed by that time. In a conference style paper, we will present our technical project involving the beginning research and overall process of delivering a final product that meets the standards of the MindTrails team, users, and NIH sponsor. By allowing a wide array of individuals to contribute, a quality product can be made to help almost a third of the population suffering from a severe anxiety disorder.

THE FUTURE OF DATA PRIVACY IN THE U.S. WITH EHEALTH INTERVENTION

Technology advances have far outpaced federal laws in the United States protecting data privacy. In the last year alone, the European Union and the State of California passed seminal legislation that defined the handling of consumers' personal information and the consequences of misuse. The U.S.'s delay in passing federal data privacy laws that protect personal data of its citizens is something that must be examined. More specifically, laws are needed to govern businesses that collect information for healthcare, especially the health care data collected on mobile devices. Deven McGraw, chief compliance officer of health tech startup Citizen, argues that the current legislation protecting health data "was never intended to cover the universe and as that universe expands, it looks less and less adequate" (Bindley, K., 2019, Gaps in the framework section, para. 1). A study conducted in 2019 found that a majority of applications concerning mental health did not have clear, readable privacy policies (PPs) or terms of agreements (ToAs) (Robillard et al.). This lack of transparency concerning companies' use of personal information caused the authors to "raise concerns about consent, transparency, and data sharing associated with mental health apps [which]…highlight the importance of improved regulation in the mobile app environment" (Robillard et al., 2019, Abstract section, para. 3). The Health Insurance Portability and Accountability Act (HIPAA) should theoretically protect user's personal health information used in these apps. However, HIPAA only covers information passed back and forth between insurance companies, doctors, and other healthcare systems.

This lack of protection comes at a time when consumers do not understand how their data is being used, especially in the field of health apps. It has already been shown that companies sell customer information – i.e., Facebook's selling of 50 million users' information to Cambridge

Analytica ("The Facebook Scandal", 2018). Other countries also have become wary of how the U.S. handles data, perhaps due to Edward Snowden leaking National Security Agency information. As a result, this information led to an Ireland ruling in 2015 which stated that "the U.S. does not actually provide sufficient protection of private data" (Finley, K., 2015, para. 4). The ruling eventually became the catalyst for enacting the General Data Protection Regulation (GDPR) three years later. As the European Union requires more detailed and transparent data usage from U.S. and EU companies, U.S. companies will need to manage all the requirements stemming from the GDPR, U.S. sector-based statues, and California's Consumer Privacy Act (CaCPA). The future is unclear in the U.S. surrounding the enactment of a singular, federal-level data privacy legislation for U.S. companies.

SENSITIVE INFORMATION LIKE HEALTH DATA REQUIRES ADDITIONAL STEPS

The matter surrounding data privacy becomes more complicated when the data is considered sensitive. In their book, Solove and Schwartz highlighted the inconsistency in the legislative language surrounding sensitive data (Voss, W.G. & Houser, K., 2019). Instead of a single legislation defining sensitive data, the U.S. has industry-based laws and regulations protecting what they view as "sensitive" data in their own way. For example, HIPAA has its own rules governing personal data. HIPAA, however, only covers certain entities like clinicians, pharmacies, and health plans, and its reach only extends to patient information. (Cohen, G & Mello, M., 2018). HIPAA, at this point in time, does not protect sensitive health information gathered from personal mobile applications. Consequently, the guidelines and regulations must be updated frequently to align with evolving technology and other newly enacted legislations. Additionally, Parker, Halter, Karliychuk, and Grundy discovered in 2019 that 41% of sampled

mental health apps do not contain privacy policies explaining the collection and use of privacy data. They concluded that "the app industry pays insufficient attention to protecting the privacy of mental health app users" (para. 1) and identified the harmful effects that could arise such as targeted advertising, exploitative personal data leakage, and emotional harm (Parker et al., 2019).

APPLYING PACEY'S TRIANGLE TO DATA PRIVACY

In order to determine who is responsible for the protection of health data, Pacey's triangle can be applied using the entirety of the data privacy ecosystem. Stakeholders can be divided into the cultural, organizational, and technical aspects of data privacy, aligning with Arnold Pacey's approach. Pacey developed a method to distinguish specific tools from the broader practices used within a discipline. Stakeholder groupings can be categorized by the knowledge, skill, and technique of each group, as illustrated in Figure 2 (Pacey, 1983). These stakeholders can be further broken down into users and the experts. Adapted from Pacey's Triangle and *The Culture of Technology,* Figure 3 on page 9 identifies different groups and practices that develop meaning from data privacy. The user sphere refers to those individuals that are affected by changes and advancement of data privacy but cannot directly enforce or design improvements. Legal activity by the government can attempt to

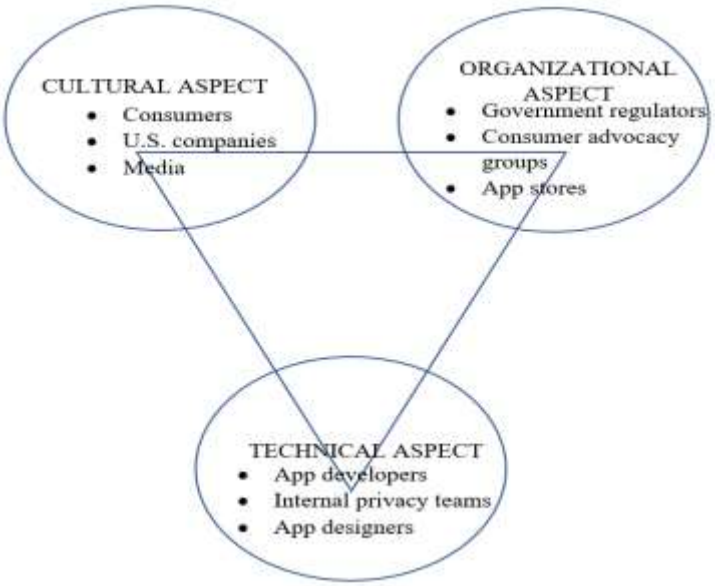

Figure 2: Pacey's Triangle for data privacy: Stakeholders are grouped into their respective categories based on how they can contribute to data privacy. Groups do not necessarily share the same meaning and values but are classified based on their overall experience and capabilities (Adapted by Anderson from Pacey, 2019).

incentivize app developers and app stores to adopt safer data collection processes by creating laws and legislation concerning users' personal data rights. Government regulators in the U.S. should advocate for similar legislation to the GDPR that better protects personal information. With regards to health data, HIPAA provides a legislative platform to drive improvements targeted to address the issues. Additionally, the government could fund app security innovation to reduce the number of data breaches and identity theft involving user data. Moreover, opportunity exists to improve app designing and planning, including the use of anonymization and pseudonymization. Pseudonymization is a technique similar to anonymizing user information, however with pseudonymization, reidentification is possible. In terms of U.S. regulation, pseudonymization can be considered a suitable addition to data security, however, for GDPR, "in order for data to be out of definition of personal data it [sic] has to be properly anonymized; pseudonymization is not enough" (Voss, W.G. & Houser, K., 2019, p. 322). Therefore, explicit instructions need to be provided to companies because of conflicting views on data security.

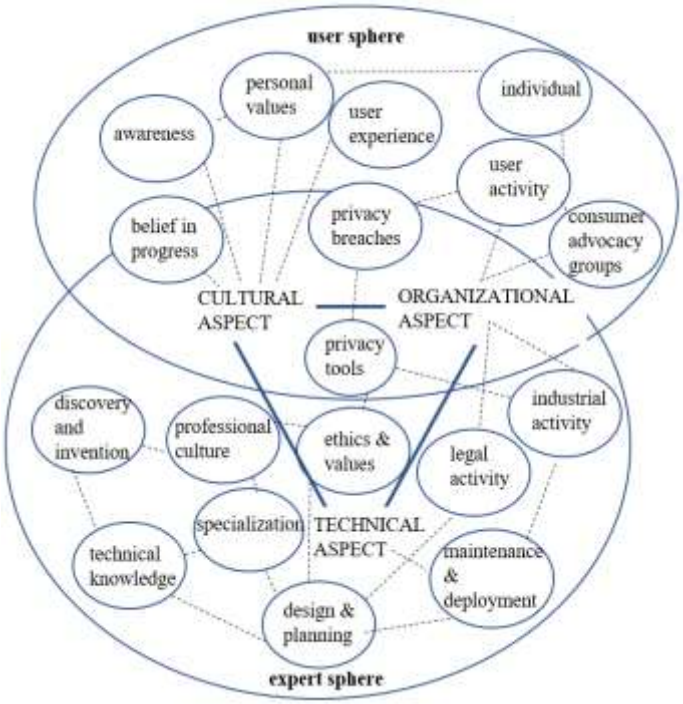

Figure 3: Technology-practice for data privacy: Users include people from outside the mobile app industry and government organizations. The user sphere encompasses all who attribute meaning from data privacy and are affected by it. The expert sphere has more control over the technology for ensuring data privacy (Adapted by Anderson from Pacey, 2019).

UPDATING HIPAA TO REFLECT CURRENT SOCIETY CHANGES

The enaction of HIPAA laws in 1996 sparked the beginning of sensitive healthcare data protection in the United States. Unfortunately, HIPAA laws were not updated to keep ahead of technology and how businesses used and protect data. Jordan Harrod, a Ph.D. student at a Harvard-MIT program, argues that the few updates throughout the years are insufficient. The first major addition to the act occurred in 2003 with the Privacy Rule, which defined personal health information (PHI) as "any information held by a covered entity which concerns health status, the provision of health care, or payment for healthcare that can be linked to an individual" (Harrod, 2019, What is HIPAA section, para. 3). However, PHI does not contain personal information collected from a user app or program like the Calm Thinking for MindTrails. The most recent add-on to HIPPA came about in 2013 with the Final Omnibus Rule. Final Omnibus further defined specific encryption standards and covered entities. Yet, HIPAA has remained unchanged in the last 7 years, and the time has come modernize U.S.'s only health legislation (Harrod, 2019). Using the GDPR as a guideline, the changes recommended for HIPAA will reflect better protection practices as well as more suitable encryption standards. Thus, this STS research project will be a scholarly article researching ways that the outdated could be refreshed. Specifically, an analysis will be conducted on the impacts of how machine learning has been able "de-crypt" the outdated encryption standards set up HIPAA. Furthermore, a close look of the GDPR will determine how health data privacy can be better protected. At this point, since HIPAA remains the only way health data is protected in the U.S., it is vital that the legislation simultaneous evolves with new technology-practices.

WORKS CITED

Anderson, Darby (2019). Figure 1: CBM-I and Implementation Intentions.

Azevedo, J., Delaney, H., Epperson, M., Jbeili, C., Jensen, S., McGrail, C.,…Barnes, L. (2019). *Gamification of eHealth interventions to increase user engagement and reduce attrition.* Paper presented at the Systems & Information Design Symposium at UVA, Charlottesville, VA.

Bandelow, B. & Michaelis, S. (2015). Epidemiology of anxiety disorders in the 21st century. *Dialogues in Clinical Neuroscience, 17*(3), 327-335. Retrieved from https://www.dialogues-cns.org/

Bindley, K. (2019, November 22). Your health data isn't as safe as you think. *The Wall Street Journal.* Retrieved from https://www.wsj.com/articles/your-health-data-isnt-as-safe-as-you-think-11574418606?shareToken=st7af4b9d50fa34e1c9f28bfb69e99b736&reflink=article_email_share

The Facebook scandal could change politics as well as the Internet. (2018, March 22). *The Economist.* Retrieved from https://www.economist.com/united-states/2018/03/22/the-facebook-scandal-could-change-politics-as-well-as-the-internet

Finley, K. (2015, October 6). Thank (or blame) Snowden for Europe's big privacy ruling. *Wired.* Retrieved from https://www.wired.com/2015/10/tech-companies-can-blame-snowden-data-privacy-decision/

Harrod, J. (2019, May 15). Health data privacy: Updating HIPAA to match today's technology challenges [Blog post]. Retrieved from http://sitn.hms.harvard.edu/flash/2019/health-data-privacy/

Harvey, A. G., & Gumport, N. B. (2015). Evidence-based psychological treatments for mental disorders: Modifiable barriers to access and possible solutions. Behaviour research and therapy, *68*, 1-12.

MacLeod, C. (2012). Cognitive bias modification procedures in the management of mental health disorders. *Current Opinion Psychiatry, 25*(2), 114-120. doi:10.1097/YCO.0b013e32834fda4a

Miloff, A., Marklund, A., Carlbring, P. (2015). The challenger app for social anxiety disorder: New advances in mobile psychological treatment. *Internet Interventions, 2,* 382-391. doi:10.1016/j.invent.2015.08.001

NAMI. (2019, September). Mental Health by the Numbers | NAMI: National Alliance on Mental Illness. Retrieved September 17, 2019, from https://www.nami.org/learn-more/mental-health-by-the-numbers

Pacey, A. (1983). *The culture of technology*. Cambridge, MA: The MIT Press.

Parker, L., Halter, V., Karliychuk, T., & Grundy, Q. (2019). How private is your mental health app data? An empirical study of mental health app privacy policies and practices. *International Journal of Law and Psychiatry, 64*, 198-204. doi:10.1016/j.ijlp.2019.04.002

Price, M., Yuen, E.K., Goetter, E.M., Herber, J.D., Forman, E.M., Acierno, R., & Ruggiero, K.J. (2013). mHealth: A mechanism to deliver more accessible, more effective mental health care. *Clinical Psychology & Psychotherapy, 21*(5), 427-436. doi:10.1002/cpp.1855

Robillard, J.M., Feng, T.L., Sporn, A.B., Lai, J. Lo, C. Ta, M., & Nadler R. (2019). Availability, readability, and content of privacy policies and terms of agreements of mental health apps. *Internet Interventions, 17*, doi:10.1016/j.invent.2019.100243

Voss, W.G. & Houser, K.A. (2019) Personal data and the GDPR: Providing a competitive advantage for U.S. companies. *American Business Law Journal*, *56*(2), 287-344. doi:10.1111/ablj.12139

Webb, T.L., Ononaiye, M.S.P., Sheeran, P., Reidy, J.G., & Lavda, A. (2010). Using implementation intentions to overcome the effects of social anxiety on attention and appraisals of performance. *Personality and Social Psychology Bulletin*, *36*(5), 612-627. doi:10.1177/0146167210367785