New Strategies to Increase Engagement and Decrease Dropout in mHealth Interventions

(Technical Paper)

How Is the Utility of Differential Privacy, a Data Protection Technique, Constructed Within the Fields of Health and Political Science?

(STS Paper)

A Thesis Prospectus Submitted to the

Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements of the Degree

Bachelor of Science, School of Engineering

R.X. Schwartz

Fall, 2021

Technical Project Team Members

Annabel Lynch

Disha Patel

Aparna Ramanan

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

Signature _____ Date _____

R.X. Schwartz

Approved _____ Date _____

Laura Barnes, Associate Professor, Department of Engineering Systems and Environment

Approved _____ Date _____

Bryn Seabrook, Assistant Professor, Department of Engineering and Society

Introduction

According to the UN's latest statistics, "global spending on R&D [research and development] has reached a record high of almost US$ 1.7 trillion" (UNESCO Institute for Statistics, n.d.). Yet how are these research innovations integrated into commercial and scientific environments? This process is often known as translation research, an area of study that focuses on methods for moving research discoveries to the external world (National Institute for Occupational Safety and Health, 2018). At the same time, not all research discoveries are easily translated into practical applications, perhaps due to economic infeasibility, low technology maturity, or a lack of demand.

Yet there are many areas in society in which the application of new research is certainly needed. In the area of mental health treatment, The World Health Organization (WHO) notes that approximately "20% of the world's children and adolescents have a mental health condition" and that "two of the most common mental health conditions, depression and anxiety, cost the global economy US$ 1 trillion each year" (World Health Organization, 2019). In the separate area of user privacy protections, Article 12 of the Universal Declaration of Human Rights declares that privacy is a protected right (United Nations, 1948); yet the UN High Commissioner for Human Rights notes that privacy is now ever more threatened by the automated processing of data, with special concern paid towards the "possibility of de-anonymization that is facilitated by fusing data from various sources" (United Nations High Commissioner for Human Rights, 2021). These concerns highlight the need for effective translation research to support mental health and protect individual privacy.

This capstone project responds to these twin challenges of mental health treatment and user privacy protections. In the technical project, new conversational agent strategies will be

considered in order to increase engagement and reduce dropout in mobile health (mHealth) interventions. In the STS research paper, the social construction of the utility of differential privacy, a data protection technique, will be examined within the specific fields of health and political science. Together, these research projects will help advance current translation research, by either directly assisting with the translation of research into practice in the mHealth field (the technical project), or by noting the areas in which privacy-related translation research may encounter difficulties (the STS research paper).

Technical Project (New Strategies to Increase Engagement and Decrease Dropout in mHealth Interventions)

Electronically mediated mental health interventions suffer from high rates of attrition, also known as user abandonment (Gabrielli et. al 2021, Pratap et. al 2020). These high rates of attrition lead a proportion of users who desire to improve their mental health through technological interventions to fail to do so, ultimately limiting the utility of the intervention. Additionally, high attrition from digital mental health interventions poses concerns for the generalizability of the intervention to a general population. In response, the technical project of the capstone focuses on new strategies to increase engagement and decrease dropout in mobile health (mHealth) interventions. Specifically, the technical project will pair these strategies with the larger MindTrails digital mental health intervention platform, hosted at the University of Virginia. The team members on this technical project will consist of Rob Schwartz, Annabel Lynch, Disha Patel, and Aparna Ramanan (students); Laura Barnes and Sonia Baee (MindTrails researchers); and potentially other researchers from the MindTrails group.

The MindTrails group has previously tested the use of human coaches to help increase engagement in the MindTrails mental health intervention system and to lessen attrition from the

platform. However, the cost of human coaches cannot be suitably scaled in digital applications that are designed to reach a large number of participants. The use of human coaches is also impractical at certain times of day and in periods in which there is particularly high demand from users for mental health support. As a result, the research conducted within the technical project will design conversational agents (CAs) in order to support user engagement and reduce attrition in the MindTrails platform. Conversational agents are programs that mimic human text-based responses in order to hold a conversation with users. For example, a CA could have a structured conversation with a user if the user encounters technical issues with the MindTrails tool.

Research on conversational agents (CAs) in digital mental health technologies faces several challenges and limitations. Although CAs have been previously deployed in digital mental health technologies, user attrition remains high (Prochaska et. al 2021, Gabrielli et. al 2021). Furthermore, CAs face an inherent tradeoff between predictability and utility: if a CA supports open-ended question and answer sessions, then it may give improper or even harmful responses; yet if a CA only allows closed-ended question and answer sessions, then it may also fail to support as-yet-unidentified user needs. These concerns cause the design and implementation of conversational agents to be a delicate area of study that also requires significant user testing and feedback.

In order to plan for the inclusion of a conversational agent in the MindTrails project, the main portion of the technical project will focus on testing the user acceptance of a conversational agent that is embedded in the MindTrails system. The CA will use a closed-ended question and answer system that is designed to support engagement on a variety of predefined topics related to mental health. (A closed-ended system will be used in order to increase predictability of responses and create an opportunity for more structured data analysis.) The research will be in

the form of a *feasibility study*, which will assess user reactions to the conversational agent using research methods that do not meet the criteria of a randomized controlled trial (RCT). Although this research will not be able to prove a causal link between the inclusion of a conversational agent and improvement of mental health conditions, this research will prepare the MindTrails project for the ultimate use of a CA in the user-facing MindTrails platform. Additionally, conclusions from this research will be of relevance to the design of other digital mental health intervention tools that use CAs.

STS Research Paper (How is the utility of differential privacy, a data protection technique, constructed within the fields of health and political science?)

Motivation and Background

Differential privacy is a relatively new data protection technique where counts of populations in publicly released datasets (such as Census data describing race, location, or ethnicity) are "fuzzed" so that the data cannot be used to re-identify individuals. For example, it may be that 20,000 individuals live in a particular US county: differential privacy would add random noise to this statistic, so that it is reported as, e.g., 21,538.6, with a standard deviation of 2,312.8 (US Census Bureau 2019). The goal of differential privacy is to protect against reconstruction attacks and re-identification attacks, which use features of datasets to learn protected information (Emam et. al, 2011). For example, certain qualities of the non-privatized 2010 Census data allowed 46% of the original dataset (that is, *individual-level* Census block id, voting age status, sex, year of birth, race, and ethnicity) to be reconstructed, which is concerning because this data can then be successfully connected to commercially available databases to identify 45% of the population by name and address (Abowd n.d.). For this reason, among others, differential privacy has been implemented in the 2020 Census dataset, as well as in

datasets in public health and other fields (US Census Bureau 2019, Google and Apple 2021, Ficek et. al 2021).

In response to the increasing use of differential privacy techniques, a portion of researchers have criticized the use of these techniques because they distort data analysis. Some of these concerns have to do with the *privacy budget* of differential privacy implementations, which refers to the amount of noise added to each statistic (Swanson and Cossman n.d.). By increasing the noise in the dataset, the power of any given statistical test will be reduced, limiting analysis of the dataset. However, the privacy budget can at times be adjusted, thereby making analysis more accurate in exchange for fewer privacy protections. Some concerns also stem from the *type* of analysis that is made inaccurate because of differential privacy techniques: one example can be seen in the 2020 Census data, in which 765 Alaskan Census blocks are suggested to contain a total of 3,381 children residing without adults (out of the 45,292 blocks in the state). In reality, the actual number of children residing without adults in the state is almost certainly magnitudes lower: in the 2010 Census, there were only three blocks that contained a total of 21 children residing without adults (Swanson et. al. n.d.). Lastly, there is some criticism that is *inherent* to the use of differential privacy in specific contexts: for example, health datasets with "limited data or small populations" may be particularly unsuitable for differential privacy techniques, according to a recent literature review (Ficek et. al 2021).

The use of differential privacy presents a conflict between users, data analysts, and privacy researchers who each want to optimize how to protect user privacy while at the same time collecting actionable data. In the meantime, this conflict is played out in research papers all around the world as the implementation of differential privacy is both supported and questioned. To analyze this discussion and understand how the utility of the differential privacy technique is

determined and shaped, this STS research paper will examine the social construction of the utility of *differential privacy*, a data protection technique, within the specific fields of health and political science. This STS research paper will focus on the health and political science fields in particular due to the increasing application of differential privacy techniques in datasets used in these fields.

The STS research paper will analyze current research literature using Bijker's STS theory known as SCOT, or the social construction of technology. SCOT rejects technological determinism, the concept that "(1) technology develops autonomously and (2) technology determines societal development to an important degree." (Bijker 2015). Instead, SCOT proposes that "the development, stabilization, and even working of technology are socially constructed" (Bijker 2015). The SCOT approach supposes that social elements can in fact be used to understand the construction of technology: in this STS research paper, the primary social evidence used to trace the construction of differential privacy and its utility will be research papers.

One criticism of the research-paper based SCOT approach is that the research papers themselves may be biased in terms of which content is surfaced or hidden. However, Bijker's response to this criticism is that the researcher still has an "obligation to decide which groups are important to include in the account, and which groups only obfuscate the picture by adding useless details" (Bijker 2015). Bijker's criticism is similar to that of Russell, who argues that SCOT does not do enough to consider the innate *structural location* of technologies in society and forgets to consider how this structural location may limit who has the chance to criticize or shape technologies (Russell 1986). Although these criticisms are compelling (and provide good arguments for the use of a broader STS approach, such as actor-network theory), one of the

strengths of the research-paper method of SCOT is its accuracy in areas where the relevant socio-technical debate is mainly conducted in and through research. Given that differential privacy is a highly technical topic that is significantly shaped by academics and data practitioners, the approach of using research papers as primary material is suitable in this case (Schneider, 2021).

Lastly, STS research into the social construction of the utility of differential privacy is important for understanding the consequences of data protection in publicly-released datasets: differential privacy techniques may protect users, limit the effectiveness of research, and/or pose equity challenges, among many other potential outcomes (Santos-Lozada et. al, 2021). By understanding the ways in which the utility of differential privacy techniques is constructed by users, data analysts, and law, designers of publicly released datasets will be better able to justify and understand the impact of their decisions when implementing differential privacy techniques.

Research Question and Methods

The STS research paper considers the research question "How is the utility of differential privacy, a data protection technique, constructed within the fields of health and political science?" The approach to answering this question will begin with a traditional literature review, which will be completed by using structured searches of online databases as well as gathering of known relevant sources from outside these databases (Stratton 2019). To find health-related literature on the social construction of differential privacy, the PUBMED database will be searched on a full-text basis using the combined terms "differential privacy" and "tradeoff." Additionally, the ACM database will be searched on a full-text basis using the combined terms "differential privacy" and "tradeoff," with health- and political-science-related articles extracted. Due to the multifaceted nature of the health and political science fields, a search on Google

Scholar will also be conducted using the combined terms “differential privacy” and “tradeoff” with health- and political-science-related articles extracted. Any known sources that are not indexed in these databases but that are known to the author and relevant to the topic will also be included. Next, SCOT will be used as a framework to identify stakeholder groups within this literature, to describe their interests, and to identify how differential privacy systems support, subvert, or suppress the interests of these groups in the process of constructing the utility of differential privacy.

As mentioned above, the literature review method is suitable for the research question at hand given that the construction of the utility of differential privacy has mainly occurred within academic fields (Schneider, 2021). The keywords “differential privacy” and “tradeoff” should be suitable for this literature review due to the heavy use of these terms within a similar literature review in the health field (Ficek et. al, 2021).

Conclusion

This portfolio will include (1) a technical project that determines the user acceptance of conversational agents within MindTrails, a digital mental health support platform, and (2) an STS research paper that considers how the utility of the data protection technique known as differential privacy has been socially constructed. Both of these papers will contribute to a more comprehensive understanding of translational research in their respective areas, identifying points of concern and success in cases where the technologies of conversational agents and differential privacy are moved from the academic sphere into practical, user-facing environments. In all, these two papers will help future academics or practitioners approach the implementation challenges faced in the mental health and user privacy areas today.

References

Abowd, J. M. (n.d.). *Tweetorial: Reconstruction-abetted re-identification attacks and other traditional vulnerabilities | John M. Abowd*. John M. Abowd. Retrieved October 4, 2021, from https://blogs.cornell.edu/abowd/special-materials/245-2/

Bijker, W. E. (2015). Technology, Social Construction of. *International Encyclopedia of the Social & Behavioral Sciences*, 135–140. https://doi.org/10.1016/b978-0-08-097086-8.85038-2

Emam, K. E., Jonker, E., Arbuckle, L., & Malin, B. (2011, December 2). *A Systematic Review of Re-Identification Attacks on Health Data*. PLOS One. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3229505/

Ficek, J., Wang, W., Chen, H., Dagne, G., & Daley, E. (2021). Differential privacy in health research: A scoping review. *Journal of the American Medical Informatics Association,* 28(10), 2269–2276. https://doi.org/10.1093/jamia/ocab135

Gabrielli, S., Rizzi, S., Bassi, G., Carbone, S., Maimone, R., Marchesoni, M., & Forti, S. (2021). Engagement and Effectiveness of a Healthy-Coping Intervention via Chatbot for University Students During the COVID-19 Pandemic: Mixed Methods Proof-of-Concept Study. *JMIR MHealth and UHealth, 9*(5). https://doi.org/10.2196/27965

Google & Apple. (2021, April). *Exposure Notification Privacy-preserving Analytics (ENPA) White Paper*. Apple. https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ENPA_White_Paper.pdf

National Institute for Occupational Safety and Health. (2018, May 1). *Translation Research | NIOSH | CDC*. Retrieved November 1, 2021, from

https://www.cdc.gov/niosh/topics/translationresearch/default.html

Pratap, A., Neto, E. C., Snyder, P., Stepnowsky, C., Elhadad, N., Grant, D., Mohebbi, M. H., Mooney, S., Suver, C., Wilbanks, J., Mangravite, L., Heagerty, P. J., Areán, P., & Omberg, L. (2020). Indicators of retention in remote digital health studies: a cross-study evaluation of 100,000 participants. *npj Digital Medicine*, *3*(21). https://doi.org/10.1038/s41746-020-0224-8

Prochaska, J. J., Vogel, E. A., Chieng, A., Kendra, M., Baiocchi, M., Pajarito, S., & Robinson, A. (2021). A Therapeutic Relational Agent for Reducing Problematic Substance Use (Woebot): Development and Usability Study. *Journal of Medical Internet Research*, *23*(3). https://doi.org/10.2196/24850

Russell, S. (1986). The Social Construction of Artefacts: a Response to Pinch and Bijker. *Social Studies of Science*, *16*(2), 331–346. https://doi.org/10.1177/0306312786016002008

Santos-Lozada, A. R., Howard, J. T., & Verdery, A. M. (2020). How differential privacy will affect our understanding of health disparities in the United States. *Proceedings of the National Academy of Sciences*, 117(24), 13405–13412. https://doi.org/10.1073/pnas.2003714117

Schneider, M. (2021, June 9). Census releases guidelines for controversial privacy tool. *AP News*. https://apnews.com/article/business-census-2020-55519b7534bd8d61028020d79854e909

Stratton, S. J. (2019). Literature Reviews: Methods and Applications. *Prehospital and Disaster Medicine*, *34*(04), 347–349. https://doi.org/10.1017/s1049023x19004588

Swanson, D. A., Bryan, T. M., & Sewell, R. (n.d.). *The Effect of the Differential Privacy Disclosure Avoidance System Proposed by the Census Bureau on 2020 Census Products:*

Four Case Studies of Census Blocks in Alaska. National Conference of State Legislatures. Retrieved October 3, 2021, from https://www.ncsl.org/Portals/1/Documents/Elections/Four_Case_Studies_of_Census_Blocks_in_Alaska.docx.pdf

Swanson, D. A., & Cossman, R. E. (n.d.). *The Effect of the Differential Privacy Disclosure Avoidance System Proposed by the Census Bureau on 2020 Census Products: Four Case Studies of Census Blocks in Mississippi*. National Conference of State Legislatures. Retrieved October 3, 2021, from https://www.ncsl.org/Portals/1/Documents/Elections/Four_Case_Studies_of_Census_Blocks_in_Mississippi.pdf

UNESCO Institute for Statistics. (n.d.). *How much does your country invest in R&D?* Retrieved November 1, 2021, from http://uis.unesco.org/apps/visualisations/research-and-development-spending/

United Nations. (1948, December 10). *Universal Declaration of Human Rights*. Retrieved November 1, 2021, from https://www.un.org/en/about-us/universal-declaration-of-human-rights

United Nations High Commissioner for Human Rights. (2021, September). *The right to privacy in the digital age: report (2021)* (A/HRC/48/31). Human Rights Council - United Nations High Commissioner for Human Rights. https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session48/Documents/A_HRC_48_31_AdvanceEditedVersion.docx

US Census Bureau. (2019, July 1). *Census Bureau Adopts Cutting Edge Privacy Protections for 2020 Census*. The United States Census Bureau.

https://www.census.gov/newsroom/blogs/random-samplings/2019/02/census_bureau_adopts.html

World Health Organization. (2019, December 19). *Mental health: Burden*. Retrieved November 1, 2021, from https://www.who.int/health-topics/mental-health#tab=tab_2