Journal of Technology in Behavioral Science
https://doi.org/10.1007/s41347-018-0049-3

BRIEF REPORT

Assessment of Risk Associated with Digital and Smartphone Health Research: a New Challenge for Institutional Review Boards

John Torous[1] · Laura Weiss Roberts[2]

Innovative offerings in digital health are growing rapidly, with more than 250,000 health-related smartphone apps available, on last count, for immediate download on the Apple iTunes or Android Google Play stores (Torous and Roberts 2017). Research efforts to establish the potential efficacy, effectiveness, and risks of these digital applications have been relatively slow. For example, only 18 randomized controlled studies of depression smartphone apps (Firth et al. 2017b) and nine randomized controlled studies of anxiety smartphone apps have been published at the time of this writing (Firth et al. 2017a). Given the mounting expectations for digital health to serve as a means of augmenting usual clinical care practices and providing access to care to underserved populations, especially in mental health (Lau and Kolli 2017; Wen et al. 2017; Joshi et al. 2017; Snow et al. 2017; Louie et al. 2017), there is tremendous need for empirical investigation of the use of smartphones in addressing health concerns (Firth et al. 2016). Failure to perform such studies means that many hundreds of thousands (soon millions) of users may be exposed to digital interventions that, at best, may not help and, at worst, may cause harm on a vast scale to vulnerable and at-risk individuals (Torous et al. 2014).

The transition of smartphone research from niche to mainstream will prompt a number of questions regarding institutional oversight of these novel human studies. Institutional review boards (IRBs) are increasingly faced with the responsibility of assessing the nature of potential benefits and risks associated with mental health digital applications. Given the evolving nature of smartphones, shifting societal norms in relation to technology, and the progression of research questions, the benefit-to-risk ratio associated with empirical studies of digital health applications cannot be captured with a simple formula. There is also currently little guidance from regular bodies such as the US Food and Drug Administration (FDA). At the time of this writing, there is only a single FDA-approved smartphone app. The FDA itself is piloting new ways to evaluate these apps with an ongoing pre-certification pilot program expected to inform future policy. Even with more guidance from the FDA, the research nature of much digital health work still requires IRB attention. IRB assessments of potential benefits, potential risks, and their relationship are important, as these assessments influence the level of oversight required to ensure scientific rigor, safety, and the protection of rights in the conduct of such studies with human volunteers.

Evaluation of Risk

Changing Consumer Expectations and Realities

A primary challenge in assessing the risk and magnitude of harm of smartphone studies is determining an appropriate benchmark or "gold standard" for comparison. If *minimal risk* is considered to be those risks encountered *in daily life*, what does this mean in the fast-paced world of mobile technology? One main risk of smartphone studies, for example, is a lack of adequate privacy, but what does digital privacy mean in daily life? In 2015, an Android smartphone app could request up to 235 different permissions to interact with certain components of a user's smartphone; 65 of these requests could allow an app to access personal information. The average app requested five different permissions (Olmstead and Atkinson 2015). Even surfing the

✉ John Torous
jtorous@bidmc.harvard.edu

Laura Weiss Roberts
LWRoberts.Author@gmail.com

[1] Department of Psychiatry and Division of Clinical Informatics, Beth Israel Deaconess Medical Center, Harvard Medical School, 330 Brookline Ave, Boston, MA 02215, USA

[2] Department of Psychiatry and Behavioral Sciences, Stanford University School of Medicine, 401 Quarry Road, Stanford, CA 94305-5717, USA

Published online: 27 February 2018

Internet with Google, in daily life, is not entirely private. In 2016, the Web giant lifted its internal ban on linking Web browsing data with personally identifiable account login information (Angwin 2016). The 2017 vote of the U.S. Senate to nullify the rule submitted by the Federal Communications Commission entitled "Protecting the Privacy of Customers of Broadband and Other Telecommunications Services" means that, in our daily life, consumer Web browsing habits can now be sold by Internet service providers without consent ("FCC releases proposed rules" 2016). When Google recently began offering smartphone-based clinical depression screening tests (the Patient Health Questionnaire 9) to anyone searching for depression, the intersection of mental health and mobile technology further entered into daily life (Giliberti 2017).

The point of these examples is not to pass judgment but note that societal expectations and even legal definitions of digital privacy are evolving rapidly and inconspicuously. It is ironic that a smartphone study that offers to keep all research-derived data private, encrypted, and secure may actually give more safety than can be expected and encountered by individuals in daily life who are not engaged in research.

Established Risk

What kinds of risk do digital devices pose in the context of digital health research? It is important to consider what types of risk are possible. Risk may be considered across four domains of potential harm: physical, psychosocial, privacy/legal, and financial (Fig. 1). Beyond these categories, risk may also be considered across a continuum of severity and likelihood.

It seems unlikely that smartphone apps could be associated with physical health and bodily harm, and yet, in 2015, a young man fell off a cliff and perished while distracted by the PokemonGo app. Additionally, a rise in automotive accidents has been ascribed to smartphone-distracted driving. There is also evidence that most smartphone-based tools are not able to appropriately respond to emergencies like a suicide attempt (Miner et al. 2016; Larsen et al. 2016), although research on this topic remains nascent. One smartphone-based intervention study that used an app to help college students drink less alcohol unintentionally caused the opposite effect when students used the app to see who could drink more (Gajecki et al. 2014). Just as any website or book can offer misleading information, mental health apps are no exception. For example, one app recommended hard alcohol as a remedy for those with bipolar disorder during a manic episode (Nicholas et al. 2015). Apps like these that are made by those without sufficient clinical experience or qualifications risk providing users with dangerous information. While the potential for physical risk and bodily harm does exist, such risk appears low and is unlikely with proper IRB review of intended study procedures, interventions, and medical content of the digital technology.

It is possible to imagine several scenarios in which psychosocial harm is caused by smartphone and other digital device-based studies. Smartphones can prompt surveys with a frequency that could be perceived as bothersome. Additionally, the need to answer a certain percentage of surveys or complete a certain percentage of tasks on a smartphone in order to receive study compensation could cause undue stress. For studies that collect passive data—signals automatically collected from the smartphone such as GPS location or call and text logs—the knowledge that they are being remotely monitored may cause research subjects further stress or anxiety. Most smartphone studies do experience subject dropout, although reports of leaving a study specifically because of psychosocial harm have never been clearly documented. Studies that allow subjects to opt out of data collection, to remove the app from their device, and to request that their data be deleted may offer protections. While psychosocial harm is possible, and, some may argue, probable, it remains an understudied topic that warrants greater attention.

Clearly, the greatest risk with smartphone research relates to privacy and legal harm. The amount of data gathered by smartphones is tremendous—up to one million data points per day per individual user. GPS data can identify where a person sleeps; call and text logs can reveal personal social networks; microphones can capture voice; Wi-Fi logs can identify which networks users connect to; and other sensors can automatically collect vast

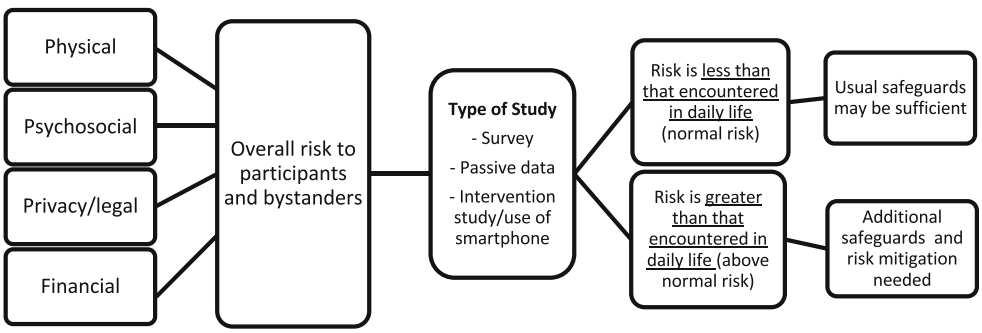

Fig. 1 Consideration of risk in IRB assessment of digital mental health research

quantities of data. A privacy breach of such data could be severe for many people, regardless of whether they have a mental health condition or not. The legal implications and harm of such data are only just becoming apparent. Earlier this year, police used fitness tracker data to bring homicide charges against an individual (Watts 2017). The risk of privacy, however, though great, is actually one of the most preventable and manageable types of risk for smartphone studies. With proper security features such as using password protection, encrypting collected data while it is temporarily on the device, securely transmitting data, securely storing data, and restricting data access, the risk of a privacy breach is minimal and less than the risk that is encountered in daily life when using online banking or sending an email, for example.

It seems unlikely that smartphone studies could cause direct financial harm, but if studies cause participants to use excessive amounts of cellular data or to wear out their own personal devices, the resulting expenses could create financial harm. This would be the case especially for those of lower socioeconomic status who rely on their smartphone as their only means of Internet connection. A 2015 Pew Poll reported that of those who relied on their smartphone as their only means of connection to the Internet, 48% had to suspend or cancel services at one point because of cost (Smith 2015). The majority of studies to date have often provided research subjects with new phones or else provided compensation for phone use. But, with a move to more population size and remote digital health studies, research will increasingly utilize participants' own personal devices. Beyond costs associated with devices, there is greater magnitude of financial harm possible if there is an unintended breach or loss of personal information, as alluded to above. Some have also raised the concern that this type of data could be used by insurance providers in the future to raise premiums or even to deny coverage to certain individuals. While financial harm is possible, the risk is low with appropriate IRB oversight.

Evolving Risks

There are several other factors worth discussing in this overview of the risk of smartphone research in the context of digital health investigation. For instance, although many know what GPS is and how it can identify a person's location, there are others who may not be as technologically literate. Researchers have reported cases of participants agreeing to smartphone-based GPS monitoring only to be shocked when they learn that GPS data can be used to determine their exact location (Nebeker et al. 2017). There is no standard assessment for technological literacy, so researchers must ensure that they educate potential volunteers adequately in order to obtain informed consent. This issue will likely grow in prominence as studies begin to utilize smartphone-based remote informed consent, which is often conducted solely through the phone, without anyone from the research team physically present. How remote informed consent compares to in-person informed consent for digital research remains an open question. Informed consent in the digital age will remain an evolving topic that IRBs must carefully consider.

Another point to consider is that of bystander rights and whether a study will collect data from those who have not consented. With the ability to record phone conversations, capture ambient sounds, take pictures, and more, it is easy to imagine that certain studies may capture data from individuals not directly partaking in the study. The numerous sensors and recording abilities of smartphones that make them such appealing research devices may also place bystanders at risk. This must be considered and evaluated.

IRBs have a duty to ensure that the data collection in smartphone studies, as well as the security features of smartphone apps, is appropriate. The risks of such studies may relate to physical harm, psychosocial harm, privacy and legal harm, and financial harm. To date, there are no systematic reports of harm to subjects associated with smartphone studies per se. Moreover, there is no evidence of any data breach from a smartphone research study. Data breaches from health apps have made national news, but research-grade apps should be more secure as many are required to undergo digital security review as part of IRB evaluation. As more companies seek to conduct clinical studies on apps, however, IRBs will likely be presented with apps with security vulnerabilities that place human subjects at risk.

A Proposed Framework

We suggest that the risk associated with mental health research involving digital technology is considered in relation to the four categories outlined in this paper: physical, psychosocial, privacy/legal, and financial. The type of risk may vary depending on the intended use of the smartphone; it is necessary to consider all four categories of risk for each intended use, while also noting the possibility for overlap. It is also important to consider what role, or roles, the smartphone or sensor technology is being employed for in the study. Using a smartphone to offer symptom surveys represents a different risk profile than using a smartphone to guide a novel therapeutic intervention. The everyday or baseline risks of using a smartphone in the same role as the study proposes should be considered. While there is no standard for baseline risk, it is useful to keep in mind what current standards and risks users face when using smartphones to communicate, to surf the Web, and to monitor their daily step count.

After considering the potential risk of a study, we suggest evaluating the likelihood and severity of that risk and assessing whether potential risks are similar to those encountered in daily life (i.e., minimal risk or greater). If the risk is greater than what is encountered in daily life, additional safeguards will absolutely be necessary for the study to be conducted ethically and in conformity with federal regulations. It is critical to ensure that risks and their likelihood and severity are well reflected in the informed consent process and conveyed in a manner that potential research subjects can understand. If necessary, this process may be repeated to evaluate risk for bystanders, depending on the nature of the proposed study and what data it may collect.

Safeguards and risk mitigation for digital psychiatry and smartphone studies remain as topics that will continue to evolve with new technologies and sensor capabilities. Looking ahead, we offer a few brief considerations. Many smartphone studies now offer programmed app responses that trigger a message or action if a certain threshold for detected or self-reported symptoms is exceeded. For example, if a research subject indicates on a smartphone survey that she is at high risk of suicide, the app can trigger a special screen offering links to help, phone numbers to call, and special instructions. The app can even be programmed to automatically alert study staff or emergency services. For longitudinal studies, especially those collecting passive data that are often out of immediate sight, it may be useful for the app to periodically prompt an on-screen reminder that the study is active and data collection ongoing. As outlined above, appropriate digital security measures are also critical. While ransomware attacks and large-scale hacking of health data continue to make global news, many of these attacks could have been prevented if industry-standard digital security measures were followed (Clarke and Youngstein 2017). In addition, resources like the U.C. San Diego Connected and Open Research Ethics platform (https://thecore.ucsd.edu/) offer free useful advice, sample protocols, and interactive forums covering ethical issues around digital health technology research. A testament to current IRB oversight is the fact that there are currently no published reports of data breaches or leaks from any mobile or digital health study.

In conclusion, smartphone and technology research for psychiatry offers the potential to advance the field with new data and insights. Such research also holds promise for improving access to health resources for millions of people. Yet, this research also brings novel research risks, and these risks are challenging to assess in a world where the risks of everyday technology use are rapidly changing and often greater than imagined. Fortunately, while the risks of smartphone studies are real, there are many ways to mitigate them and IRBs can help to keep research safe. As technology continues to evolve in psychiatry, so must our ability to apply human subject protections.

References

Angwin, J. (2016). Google has quietly dropped ban on personally identifiable Web tracking. ProPublica. https://www.propublica.org/article/google-has-quietly-dropped-ban-on-personally-identifiable-web-tracking. Accessed 30 Nov 2017.

Clarke, R., & Youngstein, T. (2017). Cyberattack on Britain's National Health Service—a wake-up call for modern medicine. *The New England Journal of Medicine, 377*(5), 409–411.

FCC releases proposed rules to protect broadband consumer privacy (2016). Federal Communications Commission. https://www.fcc.gov/document/fcc-releases-proposed-rules-protect-broadband-consumer-privacy. Accessed 30 Nov 2017.

Firth, J., Torous, J., & Yung, A. R. (2016). Ecological momentary assessment and beyond: the rising interest in e-mental health research. *Journal of Psychiatric Research, 80*, 3–4.

Firth, J., Torous, J., Nicholas, J., Carney, R., Rosenbaum, S., & Sarris, J. (2017a). Can smartphone mental health interventions reduce symptoms of anxiety? A meta-analysis of randomized controlled trials. *Journal of Affective Disorders, 218*, 15–22.

Firth, J., Torous, J., Nicholas, J., Carney, R., Pratap, A., Rosenbaum, S., et al. (2017b). The efficacy of smartphone-based mental health interventions for depressive symptoms: a meta-analysis of randomized controlled trials. *World Psychiatry, 16*(3), 287–298.

Gajecki, M., Berman, A. H., Sinadinovic, K., Rosendahl, I., & Andersson, C. (2014). Mobile phone brief intervention applications for risky alcohol use among university students: a randomized controlled study. *Addiction Science & Clinical Practice, 9*, 11.

Giliberti, M. (2017). Learning more about clinical depression with the PHQ-9 questionnaire. *The Keyword*. https://www.blog.google/products/search/learning-more-about-clinical-depression-phq-9-questionnaire/. Accessed 30 Nov 2017.

Joshi, A., Generalla, J., Thompson, B., & Haidet, P. (2017). Facilitating the feedback process on a clinical clerkship using a smartphone application. *Academic Psychiatry, 41*(5), 651–655.

Larsen, M. E., Nicholas, J., & Christensen, H. (2016). A systematic assessment of smartphone tools for suicide prevention. *PLoS One, 11*(94), e0152285.

Lau, C., & Kolli, V. (2017). App use in psychiatric education: a medical student survey. *Academic Psychiatry, 41*(1), 68–70.

Louie, A. K., Balon, R., Beresin, E. V., Coverdale, J. H., Brenner, A. M., Guerrero, A. P. S., et al. (2017). Teaching to see behaviors—using machine learning? *Academic Psychiatry, 41*(5), 625–630.

Miner, A. S., Milstein, A., Schueller, S., Hegde, R., Mangurian, C., & Linos, E. (2016). Smartphone-based conversational agents and responses to questions about mental health, interpersonal violence, and physical health. *JAMA Internal Medicine, 176*(5), 619–625.

Nebeker, C., Murray, K., Holub, C., Haughton, J., & Arredondo, E. M. (2017). Acceptance of mobile health in communities underrepresented in biomedical research: barriers and ethical considerations for scientists. *JMIR Mhealth Uhealth, 5*(6), e87.

Nicholas, J., Larsen, M. E., Proudfoot, J., & Christensen, H. (2015). Mobile apps for bipolar disorder: a systematic review of features and content quality. *Journal of Medical Internet Research, 17*(8), e198.

Olmstead, K. & Atkinson, M. (2015). Apps permissions in the Google Play store. Pew Research Center. http://www.pewinternet.org/2015/11/10/apps-permissions-in-the-google-play-store/. Accessed 30 Nov 2017.

Smith, A. (2015). US smartphone use in 2015. *Pew Research Center*. http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/. Accessed 30 Nov 2017.

Snow, C. E., Torous, J., Gordon-Elliot, J. S., Penzner, J. B., Meyer, F., & Boland, R. (2017). Use of electronic resources for psychiatry

clerkship learning: a medical student survey. *Academic Psychiatry, 41*(5), 656–660.

Torous, J., & Roberts, L. W. (2017). Needed innovation in digital health and smartphone applications for mental health: transparency and trust. *JAMA Psychiatry, 74*(5), 437–438.

Torous, J., Keshavan, M., & Gutheil, T. (2014). Promise and perils of digital psychiatry. *Asian Journal of Psychiatry, 10*, 120–122.

Watts, A. (2017). Cops use murdered woman's Fitbit to charge her husband. *CNN*. http://www.cnn.com/2017/04/25/us/fitbit-womans-death-investigation-trnd/index.html. Accessed 30 Nov 2017.

Wen, L., Sweeney, T. E., Welton, L., Trockel, M., & Katznelson, L. (2017). Ecouraging mindfulness in medical house staff via smartphone app: a pilot study. *Academic Psychiatry, 41*(5), 646–650.