Mobile Technology for Adaptive Aging

PROCEEDINGS OF A WORKSHOP

Board on Behavioral, Cognitive and Sensory Sciences

Division of Behavioral and Social Sciences and Education

The National Academies of
SCIENCES • ENGINEERING • MEDICINE

THE NATIONAL ACADEMIES PRESS
Washington, DC
www.nap.edu

THE NATIONAL ACADEMIES PRESS 500 Fifth Street, NW Washington, DC 20001

This activity was supported by contracts between the National Academy of Sciences and the U.S. Department of Health and Human Services, Contract No. HHSN263201800029I/HHSN26300035. Support for the work of the Board on Behavioral, Cognitive, and Sensory Sciences is provided primarily by a grant from the National Science Foundation (Award No. BCS-1729167). Any opinions, findings, conclusions, or recommendations expressed in this publication do not necessarily reflect the views of any organization or agency that provided support for the project.

International Standard Book Number-13: 978-0-309-68086-8
International Standard Book Number-10: 0-309-68086-7
Digital Object Identifier: https://doi.org/10.17226/25878

Additional copies of this publication are available from the National Academies Press, 500 Fifth Street, NW, Keck 360, Washington, DC 20001; (800) 624-6242 or (202) 334-3313; http://www.nap.edu.

Printed in the United States of America

Suggested citation: The National Academies of Sciences, Engineering, and Medicine. (2020). *Mobile Technology for Adaptive Aging: Proceedings of a Workshop*. Washington, DC: The National Academies Press. https://doi.org/10.17226/25878.

1

Trust, Privacy and Security, and Accessibility Considerations When Conducting Mobile Technologies Research With Older Adults

Jessica Vitak and Katie Shilton[1]

INTRODUCTION AND OVERVIEW

Information and communication technologies (ICTs)—including smartphones, tablets, and other mobile devices—provide a number of important social, emotional, and tangible resources to older adults. Aging is associated with increased social isolation and a subsequent decline in emotional well-being; ICTs may provide a social lifeline to those living in retirement communities or far from family (e.g., Brewer and Jones, 2015; Cotten et al., 2017; Gatto and Tak, 2008). ICTs can help older adults become more cognitively engaged through games, information seeking, and other activities (Koo and Vizer, 2019; Lu et al., 2017). As physical health and mobility decline, use of mobile devices provide older adults with more freedom by removing the geographical constraints associated with many normal activities, including grocery shopping, banking, and accessing medical records (Kötteritzsch and Weyers, 2016; Winstead et al., 2013). Finally, mobile devices can help caregivers and medical staff provide better care through monitoring and data collection (Kang et al., 2010; Kuerbis et al., 2017).

While older adults generally lag behind the general population in adopting new technologies, they represent an increasingly large proportion of users. In 2019, 91 percent of American adults age 65+ owned a mobile phone and 53 percent owned a smartphone (Pew Internet, 2019). Companies are increasingly designing and marketing mobile technologies

[1]College of Information Studies, University of Maryland, College Park. Address correspondence to: jvitak@umd.edu and kshilton@umd.edu.

toward older adults to help them age in place, stay connected with family and friends, and maintain a sense of independence. Likewise, existing technologies like wearables (e.g., fitness trackers) and personal digital assistants (e.g., Amazon Echo, Google Home) can be particularly helpful to older adults as they seek to maintain their health and live on their own (e.g., Nath et al., 2018).

Mobile technologies also provide researchers with a wide range of tools and methods for doing research with older adults. Sensors, mobile apps, digital assistants, and other technologies can collect passive and active data from users to improve care, provide assistance, and enhance their quality of life, and researchers have used such technologies to develop mobile health interventions for a wide range of physical and emotional health outcomes (Joe and Demiris, 2013). These devices can also help offset problems of accuracy and recall in data collection by providing "just-in-time" data collection through text messages, apps, and other mobile tools (Heron and Smyth, 2010).

At the same time, the use of mobile technologies by older adults introduces challenging privacy and security risks. The privacy and security of mobile data is a complex topic. Mobile devices gather a broad spectrum of data about their users, ranging from in-application activity to communications to movement and location data generated by sensors in the phone, and that data is collected in ways that are not always clear to end users. For example, many applications on smartphones—including GPS/navigation, ride services, and fitness tracking—require location data to function, and many consumers will therefore opt-in (or decline to opt-out) of widespread location tracking by their device. Location data can provide an exact accounting of where a person is located at any given time and is generally considered highly sensitive (Boshell, 2019). Beyond location data, people use their phones to generate and share sensitive data, including emails, text messages, and financial transactions, which could pose privacy and security risks.

Furthermore, the sensitive data generated by mobile devices is shared with a wider ecosystem that includes device manufacturers, telecommunication companies, and application companies, as well as third party data brokers (Shilton, 2009). Although recent legislation in Europe and California provides individuals specific rights over their data, understanding those access and control rights is challenging—and which companies and researchers must adhere to the new regulations is still being fought over in the courts. And while application developers frequently give users choices about the privacy and security of their data, these choices can be cognitively and logistically difficult to navigate (Kelley et al., 2012; Madden, 2012).

Researchers collecting and/or analyzing data from mobile devices, particularly those working with older adults, must account for a wide range

of physical and cognitive abilities and tailor study design and participant protections to account for that variance. As Farage and colleagues (2012) note, designing for older adults should focus on simplicity, flexibility, and ease of use. In the case of mobile devices, this means considering how the size of the device and any text-based displays may create additional barriers to adoption and use and offering multiple formats for presenting and collecting data. Second, older adults are frequently less experienced users of mobile and digital technologies, and experience with these technologies is correlated with both trust in the systems as well as understanding of the privacy and security risks. Research suggests that older adults are more likely to experience fear or distrust of technology (Knowles and Hanson, 2018); this may lead to a lack of engagement or non-participation from some older adults (Waycott et al., 2016). Other research suggests older adults may engage in impression management strategies during the research process to counter stereotypes about older adults' knowledge of technology or provide socially desirable responses (Franz et al., 2018).

Because of the general risks to privacy and security from mobile devices, the specialized risks of research using mobile data streams, and the particular challenges of doing research with older adults, researchers at this intersection have an obligation to carefully consider their study design, paying particular attention to data collection, analysis, sharing, and storage policies. The relationship between these challenges is highlighted in Figure 1-1 below.

To guide this process of recognizing and responding to the specific challenges of conducting mobile device research with older adults, this paper first reviews general privacy and security risks in the mobile data ecosystem. It then narrows its scope to the ways those general risks intersect with research among older adults, and maps best practices throughout the research lifecycle to address these barriers. The paper also discusses the benefits and barriers to academic-corporate research partnerships in this space.

PRIVACY AND SECURITY CHALLENGES IN THE MOBILE ECOSYSTEM

The unique privacy and security challenges of the mobile ecosystem have been extensively detailed in previous work (Boyles et al., 2012; Christin et al., 2011; Decker, 2008; Future of Privacy Forum, 2012; Greene and Shilton, 2017; Harris, 2013), and researchers should be aware of these challenges before asking older adults to engage in mobile device research.

First, mobile devices collect extremely intimate data, making them very useful for research but challenging for privacy and security. Data collected from mobile devices might document who a user contacts via voice or text, how frequently, and the content of those messages; a variety of leisure

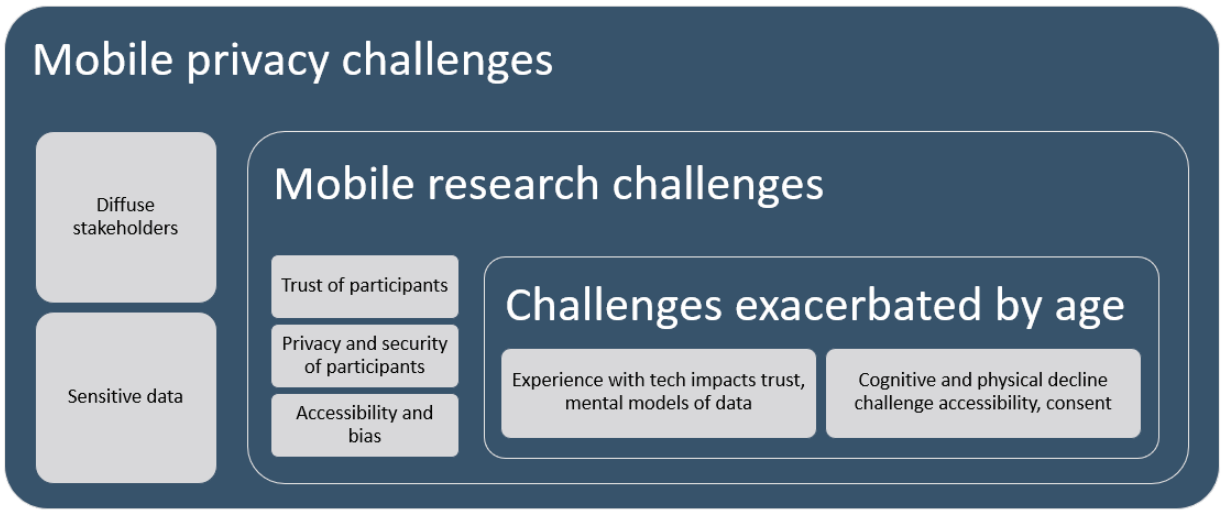

FIGURE 1-1. Nested ethical challenges of conducting mobile research with older adults.

activities ranging from shopping to games to reading; and the location of a user's home and work, as well as any other stops they make along the way. Mobile phones and wearables can intuit sleep and wake times, document searches for symptoms or concerns, and record social media activity. In most cases, the data is synced with external servers automatically, requiring no input from the user; while this improves user experience, people may easily forget—or not realize—the digital traces they share with companies throughout each day.

Next, both privacy and security of mobile data is complicated by the sheer number of data stakeholders in the mobile ecosystem. Application developers—who might range from individuals to academic researchers to huge corporations—make choices about what data to collect, how long to keep it, and how well to secure it. They may also decide to monetize user data by selling it to third-party data brokers or advertising companies. These decisions are subject to soft regulation from application marketplaces (Greene and Shilton, 2017), which generally require that users be notified of—and consent to—data collection (a minimum bar for privacy). Similar data may also be collected by device manufacturers and telecommunications companies in addition to application developers. While consumers in Europe and California have increasing rights to both the visibility of their data and restrictions on its sharing—and the U.S. Congress has been debating new privacy legislation throughout 2019—these laws are quite new (and in the case of U.S. federal legislation, still in draft form), and enforcing compliance will remain an ongoing hurdle for the foreseeable future.

Until consumer legislation is strengthened, enforced, and universally applied, researchers should be aware that asking older adults to increase data collection on mobile devices may put data into the hands of unknown third parties ranging from telecommunications companies to shadowy data brokers. Careful mobile application design can mitigate some, but not all, of these concerns. See work by the Center for Democracy and Technology (2011) and the Future of Privacy Forum (2012) for detailed recommendations on creating privacy policies and disclosures, ensuring accessibility of content, notifying end users about changes in data collection practices, sharing data with outside parties, and more.

Challenges for Mobile Data Research with Older Adults

U.S. researchers doing mobile device research with older adults have an obligation to fully inform participants of the implications of research participation, protect participants from the risks of participation, and ensure equitable access to research (Federal Register, 2017). Similar obligations apply to researchers in Canada, the UK, Australia, and the EU. However, characteristics of the research population intersect with the general chal-

lenges of mobile privacy and mobile device use in ways that particularly challenge informed consent, risk, and equity.

Privacy is frequently defined in both legal and commercial sectors as individual control over personal data (Solove, 2010). However, empirical and legal research increasingly challenges this definition (Nissenbaum, 2009; Martin and Nissenbaum, 2016). This research emphasizes privacy as the *appropriate* use of data within a given social or societal context, where appropriateness is governed by established values and social norms of a context.

We argue that avoiding a definition of privacy focused on individual control over data is particularly important for mobile data research with older adults. Ensuring privacy by asking participants to make complex decisions about the uses of their data introduces high cognitive and logistical overhead to a project, and places the burden for privacy protection on participants rather than researchers. This is inappropriate for any research, but particularly for research with older adults. Because older adults are frequently less experienced users of mobile devices, they may have incomplete mental models of what mobile data can be used to infer, who might access that information, and what the real risks of engaging in mobile data research might be.

According to a national study of American adults by Pew Internet (Auxier et al., 2019), the majority of Americans report having little to no knowledge about what companies or the government do with data they collect; furthermore, Americans generally feel they lack control over who can collect personal data. Compared to younger adults, older Americans report feeling less in control over their location data, search terms, online purchases, browsing behaviors, text messages, and social media posts (Auxier et al., 2019). At the same time, older adults are much less likely to believe their online and mobile activities are tracked than younger adults, which may lead them to make less-informed decisions about sharing personal data (Auxier et al., 2019).

These challenges of experience and understanding may impact older adults' trust in the research process and willingness to participate. In addition, age-related cognitive and physical decline may impact both the accessibility of research projects for participation, and participants' ability to meaningfully consent to complex, granular data collection. The following sections discuss challenges to informed consent and trust, privacy and security risks, and accessibility and bias, and suggest best practices to mitigate concerns in each area.

Addressing Challenges to Informed Consent and Trust

Trust is a critical component in any research setting, but becomes even more important in situations where there may be knowledge or power gaps,

such as when conducting technology-based research with older adults. For example, Serrano and colleagues (2013) looked at the use of mobile devices for collecting health data and found that older adults were less willing to share data through mobile devices; more broadly, study participants were less willing to share sensitive health data over mobile devices compared to non-digital methods. Research also indicates that distrust in big data research is an even larger issue among marginalized communities; in a large study in the United States, Madden et al. (2017) found that older Americans with lower levels of income and education expressed greater concerns about information (and physical) privacy and security. Similarly, communities already targeted for increased surveillance (e.g., foreign-born Latinxs in the U.S.) recognize that participation in pervasive tracking could put them at greater risk.

A careful informed consent process is critical to building trust with mobile research participants. With improvements in mobile data collection and analysis techniques, researchers and ethics review boards are debating best practices for obtaining informed consent (see, for example, Vitak et al., 2016, 2017). In the U.S., new guidance from the Office for Human Research Protections emphasizes the allowability of electronic consents (eConsent) but has specified that it may not be appropriate for populations who "have difficulty navigating or using electronic systems because of, for example, a lack of familiarity with electronic systems, poor eyesight, or impaired motor skills"." (U.S. Department of Health and Human Services et al., 2016, p. 4). Informed consent—whether paper-based or electronically mediated—is further complicated because a large amount of data is being collected in the background by sensors, mobile phones, and application programming interfaces (APIs). This raises questions about both breadth and duration of data being collected, as well as whether participants can fully understand the inferences that can be made from granular data, and the resultant risks such data poses. While popular press accounts (e.g., Valentino-DeVries et al., 2018) are gradually educating consumers about the risks of device use and data collection, older adults with less technology experience may still find such inferences surprising.

An additional challenge is determining when informed consent to *existing* data use is needed at all. Studies that scrape content from social media platforms or online communities, or those that use data already collected by commercial mobile applications, raise questions about whether secondary consent for research is needed. Research by Vitak and colleagues (2016, 2017) highlights disagreements among the research community over whether informed consent for such projects is feasible, as well as variations in how institutional review boards (IRBs) in the U.S. evaluate research using large datasets.

Best Practices for Obtaining Meaningful Informed Consent

Guaranteeing meaningful informed consent for older adults is not a simple matter. The first challenge is to maximize older participants' comprehension of the study's procedure, risks, and benefits. Research with adults has shown that comprehension of standard informed consent processes is frequently low (Nishimura et al., 2013), and older adults are less likely to fully understand data collection practices involving mobile devices (Choi and DiNitto, 2013; Schreurs et al., 2017). Overly technical descriptions of data collection and analysis procedures are especially problematic for older adults because research has consistently shown that they lag behind the general population in digital literacy and skills and may lack the support network to assist them in developing those skills (e.g., Schreurs, Quan-Haase, and Martin, 2017; Wagner, Hassanein, and Head, 2010).

There are several options for maximizing comprehension during the informed consent process of any study. In order to ensure participation includes older adults with cognitive impairments, researchers should develop study materials to allow proxies to assist participants in completing the study, interact with participants across multiple sessions, and provide clear benefits for participation (Bonnie, 1997). When possible, consent should be conducted in person and the document should be readable—both in document design and complexity of text. Relying on mobile consent procedures introduces additional risks that older adults may not be able to easily navigate documents or read and comprehend materials, and should be avoided. Researchers might consider visualizing examples of the data they are collecting and clearly listing the sorts of inferences they plan to draw. Researchers should also consider analogies that can help inexperienced mobile device users to build better mental models of how the devices collect data and what it can reveal about participants. Offering alternate versions of the consent document, including audio and/or video versions of the consent information, may be useful for participants with vision or other disabilities.

In addition to having formal consent documentation, researchers may want to create a second document that provides a straightforward list of risks and benefits to participation, as well as options for discontinuing participation or having their data removed from the dataset. Even if content is written at an appropriate reading level, older adults may need additional time to read through study materials and may have questions for researchers (Alt-White, 1995). In some cases, researchers should carefully consider whether a potential participant has the cognitive capacity to make decisions regarding participation (Kim et al., 2001); in cases where a proxy is used, researchers should still try to obtain assent from the participant.

Best Practices for Building Trust with Research Participants

There are several ways to build trust in mobile data research beyond the informed consent process. First, we encourage investigators to reflect on questions of data ownership. Data ownership is a complex legal and social issue. Currently, technology users have little legal ownership over data produced by platforms and technologies due to terms of service contracts that give ownership to companies; we advocate a different model for researchers. Researchers should consider writing consent documents so that older adults understand themselves to be the primary guardians of their data. For older adults who may struggle to feel empowered in their technology use, framing their data as an asset they control and contribute can increase their sense of ownership in the research.

Researchers can also improve the trust of older participants in their project by focusing on the utility of mobile research for this demographic. Research shows that older adults may perceive newer technologies as unnecessary and are less likely to take the effort to learn about them (Lee and Coughlin, 2014; Turner et al., 2007). By engaging participants in discussions of why mobile devices are a uniquely useful and effective research tool, researchers can build participant trust and engagement in the process.

Next, we suggest investigators think of consent for older adults as an ongoing informational process, rather than a single occurrence. Because older adults may struggle with incomplete mental models of how data are collected, stored, and analyzed, researchers should look for ways to make sure that participants understand 1) data flows and 2) research process and goals *throughout the study*. This might include the use of large icons or pop-up reminders on the mobile device interface to indicate ongoing data tracking; providing a dashboard for participants to view some or all of their collected data; or providing regular project communications and updates tailored to your research population. In one example of this, Barros and colleagues (2014) describe testing a smartphone app that encouraged physical activity; in their study, they ran three rounds of data collection, making adjustments to the app's interface after each round of data collection based on feedback from older adult participants. Researchers should also consider ways to give older participants control over data collection, including the ability to turn collection on and off, or to delete data before sharing it with researchers.

We also encourage investigators to consider more participatory forms of research. Citizen science techniques for engaging participants throughout the research process can include opportunities to co-design activities for data collection apps, focus groups to engage participants in setting research goals and developing research questions, and opportunities for individuals to analyze their own data and see their data compared to others in the study

(Pandya, 2012). These techniques are particularly effective with older populations, who may have more time available to participate in co-research activities, and who can particularly benefit from the technology literacy such engagement sessions can provide.

Finally, researchers can build trust with participant populations by behaving in a trustworthy manner with participants' data. We suggest adhering to *privacy by design* as a project goal. Privacy by design is an orientation toward research and technology development that emphasizes privacy as built into every element of a technology or protocol (Cavoukian, 2012). Ensuring that privacy is embedded into study design and any technologies developed for the study is a multi-step process, which we describe in more detail in the next section.

Addressing Privacy and Security Risks in Mobile Research with Older Adults

Practicing data privacy and security by design in mobile data research with older adults involves attention to protecting participants' data at each stage of the data lifecycle: collection, storage, analysis, and deletion. We encourage researchers to craft a *data management plan* (Michener, 2015) to proactively spot privacy and security issues in their own projects and make plans to counter the issues. A data management plan for managing the data of older adults will likely not vary greatly from those for other adults; the technical means of securing sensitive data are similar across populations. However, because of the differences in expertise between researchers and older adults discussed earlier, researchers using mobile data about older adults have an increased duty of care for participant privacy and security.

Two major issues to consider during data collection are data minimization and dealing with personally identifiable information (PII). Data minimization is collecting only what is needed to answer the project's research questions. A key strategy for minimizing data collection is careful reflection on meaningful indicators. For example, is collecting a participant's location needed for an exercise monitoring project if accelerometer data is collected? Collecting the bare minimum of data needed to satisfy a project's research questions minimizes the amount of data that could be exposed in a leak, used for re-identification, or shared by third parties. Researchers should also consider performing data processing on the mobile device when possible, sending only aggregated data or models to project servers. For example, instead of collecting all location data from older adults, researchers might consider using the mobile device to process GPS readings into "time at home" and "time away from home" and keeping only those aggregate characteristics while discarding the GPS trace. Collecting and sharing a minimal set of data can reassure older adults who may treat expansive data collection with suspicion or confusion.

Next, reflect upon what data a project will collect that could be considered PII. In a world of big data and linkable datasets, "personally identifiable" has become a broader term than names or social security numbers. For example, individuals might be identifiable through their location traces, particularly those who spend large amounts of time at an identifiable home or institutional address. Individuals also may be identifiable through aggregation of several data types; for example, Sweeney (2000) showed that combining gender, birthday, and zip code is often enough to identify someone. Even de-identified data is subject to reidentification attacks when it is combined with publicly available datasets (Narayanan and Shmatikov, 2008). Researchers should realize that few people—and especially older adults—fully realize the extent of re-identifiability of mobile data. Even if investigators have taken pains to minimize the amount of PII collected, they should not rely upon de-identification of mobile data as the main privacy or security safeguard, and they should not make inflated promises of confidentiality or anonymity to project participants.

Considerations for data storage can impact the data's security. Best practices for all populations, but particularly vulnerable populations such as older adults, include encrypting data in storage on both devices and project servers, and limiting researcher access to that data. Projects should also consider access restrictions and storage protections for the application on participants' mobile devices. Storage protections such as passwords or lock codes on mobile devices have tradeoffs for research among older adults. Secure passwords become more difficult to use as memory declines with age (Kowtko, 2014). Likewise, biometric identifiers such as fingerprint unlocking available on smartphones are easy to use, but may have higher rates of failure among older adults (Kowtko, 2014). A recent study found pattern-based authentication techniques to be most usable among older adults (Grindrod et al., 2018).

Privacy measures can also be taken during data analysis. Most researchers already take steps to protect individuals in a dataset, commonly by reporting results in the aggregate. With the increased push by federal agencies and others to share data more widely—which supports a number of important research goals around replication and advancing science—new challenges arise to protecting individuals within a dataset. Researchers have consistently shown that standard de-identification techniques, such as removing sensitive variables from a dataset, do not effectively prevent re-identification of individuals (see Ohm, 2009, for a review). Furthermore, as more variables are removed from a given dataset, its utility decreases, making this process a less-than-optimal solution for advancing research. The current state of the art in technical privacy solutions is known as *differential privacy*, a technique that "ensures that the removal or addition of a single database item does not (substantially) affect the outcome of any analysis"

(Dwork, 2011). Differential privacy is especially useful for protecting datasets that will be shared more widely because it allows for robust analyses without putting individuals at risk of re-identification. See Cheruvu (2018) for a high-level overview of how differential privacy works.

Finally, researchers should plan for how data will be deleted at the end of a study. This includes managing deletion of data stored on participants' devices as well as any data on servers or in the cloud. If complete deletion is difficult or impossible due to the number of intermediaries who have stored the data, this limitation should be clearly specified to participants during the consent process. Researchers should also consider whether they will allow participants to actively delete data (or request data deletion) during the study itself. Older adults may need particular guidance on user interfaces for deleting data or requesting data deletion.

Addressing Challenges of Bias in Research With Older Adults

For researchers using mobile devices and mobile data collection, concerns extend beyond the privacy and security risks of mobile data. Study design reliant on mobile technology may also introduce issues of accessibility and bias. In this section, we discuss challenges to accessibility and bias in studies with older adults and mobile technologies.

It is important that researchers carefully evaluate their study design and materials for biases and stereotyping. When studying technology adoption and use, stereotypes abound regarding older adults aptitude, use of, and attitudes toward ICTs. Wandke and colleagues (2012) identified six myths regarding older adults and technology use, including the belief that older adults are not interested in using ICTs and view them as useless, as well as the belief that older adults lack the physical and cognitive capabilities to use ICTs. These types of assumptions could negatively bias sampling (e.g., avoiding adults 80+ or in nursing homes), protocol materials (e.g., not asking participants about certain technologies, not having them directly interact with ICTs), or interpretation of findings (e.g., making generalizations about all older adults).

It is also important for study design to minimize any effect that stereotypes held by older adults regarding ICTs may have on their participation. Older adults may be hesitant to use mobile technologies because of a lack of experience or negative past experiences (see, for example, Comunello et al., 2017). Both attitudes may negatively affect older adults' willingness to participate in research on mobile devices as well as how they interact with technologies, so researchers should consider ways of framing their study and any artifacts that might be used in the study to address these attitudes.

Finally, for researchers using existing data by partnering with mobile companies or platforms, considerations of the representation of older adults

in mobile datasets is an issue. Though the penetration of mobile devices among older individuals is increasing, just over half of U.S. adults 65 and older owned a smartphone in 2019 (Pew Internet, 2019). Almost half of all seniors in the U.S. would be left out of many existing datasets, and those left out of the data may also be marginalized in other ways.

BEYOND DATA COLLECTION: CONSIDERATIONS FOR ACADEMIC-CORPORATE PARTNERSHIPS

As noted above, numerous companies are involved directly or indirectly in developing hardware, software, and other mobile tools for older adults, and the rich data these tools collect could advance our understanding of older adults' relationship with mobile technologies. Therefore, we encourage researchers and companies to focus on collaborations that enable academic researchers access to corporate data that would be difficult—if not impossible—to obtain otherwise. Partnerships with major companies like Apple, Google, and Microsoft could advance research on a wide range of health and wellness outcomes for older adults, improving quality of life for both those aging in place and for caregivers providing assistance as adults age.

That said, we acknowledge there are significant barriers to researcher-industry collaborations that must be overcome, including corporate concerns about intellectual property and academic concerns about data access restrictions. In the aftermath of controversies which blurred the lines between corporate and academic uses of data, from Facebook's "emotional contagion" study (Selinger and Hartzog, 2016) to the revelations of improper data usage by Cambridge Analytica (Confessore, 2018), companies may be cautious about partnering with external researchers. In addition, companies may hesitate to partner with external researchers because of concerns related to research output, particularly any output likely to be critical of the company itself. Because of this, many companies may only partner with academics they already trust and require corporate sign-off of any data analyses or written reports.

In spite of these challenges, academic-corporate research partnerships are critical because of the quantity and quality of data; these companies have highly granular and longitudinal data that can be used to draw inferences and improve a range of outcomes. Given that a large percentage of the mobile technologies older adults use are targeted directly or indirectly at health and well-being, researchers can use data from mobile apps, wearables, and other devices to directly improve the health of and care for older adults. Furthermore, academic researchers can more narrowly focus on specific research questions and applications of the data that companies may have neither the time, energy, or expertise to pursue.

The biggest hurdles to overcome in data sharing between companies and academics are ensuring the privacy and security of end-user data and meeting any legal requirements set out in the company's terms of use. The recent breakdown of Facebook's partnership with independent research commission Social Science One—a program that invited researchers to submit proposals to study misinformation and promised to share aggregated data related to elections with funded researchers—highlights how challenging secure data sharing can be at scale (see Alba, 2019, for an overview). In response to concerns about Facebook releasing sensitive personal information of users, the company began applying differential privacy algorithms to the data to ensure usability and privacy; however, as of fall 2019, Facebook and Social Science One have not been able to meet these competing demands. Other research by the Future of Privacy Forum (2017) suggests that while there are signs that companies are more open to academic partnerships, as of now they are largely limited to a small set of elite institutions and researchers. Companies are more likely to support research proposals that support the company's core mission, which may exclude important societal questions that fall outside of those goals.

Models for how corporate-academic partnerships can function do exist, and these could be used to guide future partnerships. Focusing on the role of mobile data in improving older adults' health outcomes, we can look at Apple's HealthKit and ResearchKit[2] as examples of applications that encourage individuals to voluntarily share their data with researchers and thus provide a platform for researchers to securely access and analyze that data. HealthKit is a developer framework embedded in Apple's mobile (iOS) and Watch (watchOS) operating systems that lets users share various types of data from the devices and third-party apps in an easy-to-read format through a dashboard. Individuals who want to participate in research studies can easily share their health data and can control the types of data they share. Apple's ResearchKit allows medical researchers to collect and analyze detailed and granular data from their patients unobtrusively through iPhones. Other organizations and applications have provided similar access to researchers; for example, the online platform PatientsLikeMe has procedures for allowing academic researchers to request access to their data.[3]

Recognizing that access to corporate data is difficult and may not be possible, non-profits have begun to develop guidelines and frameworks to help researchers in their evaluation of mobile technologies. One example of this PsyberGuide,[4] a non-profit organization focused on improving mental

[2] For more information, see: https://developer.apple.com/healthkit/ and https://www.apple.com/researchkit/.

[3] For more information, see: https://www.patientslikeme.com/research/faq#qr3.

[4] For more information, see: https://psyberguide.org.

health outcomes; it says its goal is to "provide accurate and reliable information free of preference, bias, or endorsement." PsyberGuide evaluates mental health apps' usability, credibility, and privacy practices and can help researchers make decisions about what mobile apps to use in their research. Other non-profits like the Future of Privacy Forum can help researchers forge new relationships with companies and help companies navigate the privacy risks associated with data sharing.

CONCLUSION

Performing research with older adults using mobile technologies places researchers and participants at a nexus of complex ethical issues. General concerns about the privacy, security, and accessibility of the mobile data ecosystem are exacerbated by the duty of care researchers owe to participants and the complex challenges of aging. In this paper, we have highlighted a number of issues researchers should consider when conducting research in this space. Our suggestions focus on ensuring accessibility and access for participants with a wide range of potential physical and cognitive limitations, reducing potential bias in research, and building trust throughout the research process. We provide specific suggestions for protecting participant data during and after data collection and communicating procedures effectively to older adults throughout the process. We advocate for researchers to embrace "non-traditional" research methods, such as employing citizen science methods of data collection to both empower older adults and provide them with more control over their data. Finally, we encourage researchers to continue to develop relationships with companies and other organizations that can enable collection and analysis of richer datasets and provide more meaningful insights into the core research questions guiding this research community.

REFERENCES

Alba, D. (2019, September 29). Ahead of 2020, Facebook falls short on plan to share data on disinformation. *The New York Times*. Available: https://www.nytimes.com/2019/09/29/technology/facebook-disinformation.html.

Alt-White, A.C. (1995). Obtaining "informed" consent from the elderly. *Western Journal of Nursing Research, 17*, 700–705. https://doi.org/10.1177/019394599501700610

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019). *Americans and privacy: Concerned, confused and feeling lack of control over their personal information*. Washington, DC: Pew Internet Project. Available: https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

Barron, J.S., Duffey, P.L., Byrd, L.J., Campbell, R., & Ferrucci, L. (2004). Informed consent for research participation in frail older persons. *Aging Clinical and Experimental Research, 16,* 79–85. https://doi.org/10.1007/BF03324536.

Bonnie, R.J. (1997). Research with cognitively impaired subjects. Unfinished business in the regulation of human research. *Archives of General Psychiatry, 54*, 105–11.

Boshell, P.M. (2019, March 25). The power of place: Geolocation tracking and privacy. *Business Law Today.* Available: https://businesslawtoday.org/2019/03/power-place-geolocation-tracking-privacy/.

Boyles, J.L., Smith, A., & Madden, M. (2012). *Privacy and data management on mobile devices*. Washington, DC: Pew Internet & American Life Project. Available: http://www.pewinternet.org/Reports/2012/Mobile-Privacy.aspx.

Brewer, R.N., & Jones, J. (2015). Pinteresce: Exploring reminiscence as an incentive to digital reciprocity for older adults. *Proceedings of the 18th ACM Conference Companion on Computer Supported Cooperative Work & Social Computing* (pp. 243–246). New York: ACM. https://doi.org/10.1145/2685553.2699017.

Cavoukian, A. (2012). *Operationalizing privacy by design: A guide to implementing strong privacy practices*. Office of the Privacy Commissioner of Canada, Ontario, Canada. Available: http://www.privacybydesign.ca/index.php/paper/operationalizing-privacy-by-design-a-guide-to-implementing-strong-privacy-practices.

Center for Democracy and Technology. (2011). *Best practices for mobile applications developers*. Available: http://www.cdt.org/blogs/2112best-practices-mobile-applications-developers.

Cheruvu, R. (2018, November 19). A high-level introduction to differential privacy. *Towards Data Science* (blog). Available: https://towardsdatascience.com/a-high-level-introduction-to-differential-privacy-edd20e6adc3b.

Choi, N.G., & DiNitto, D.M. (2013). The digital divide among low-income homebound older adults: Internet use patterns, eHealth literacy, and attitudes toward computer/Internet use. *Journal of Medical Internet Research, 15*(5), e93. https://doi.org/10.2196/jmir.2645.

Christin, D., Reinhardt, A., Kanhere, S.S., & Hollick, M. (2011). A survey on privacy in mobile participatory sensing applications. *Journal of Systems and Software 84*, 1928–1946. https://doi.org/10.1016/j.jss.2011.06.073.

Comunello, F., Fernández Ardèvol, M., Mulargia, S., & Belotti, F. (2017). Women, youth and everything else: Age-based and gendered stereotypes in relation to digital technology among elderly Italian mobile phone users. *Media, Culture & Society, 39*, 798–815. https://doi.org/10.1177/0163443716674363.

Confessore, N. (2018, April 4). Cambridge Analytica and Facebook: The scandal and the fallout so far. *The New York Times*. Available: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

Cotten, S.R., Yost, E., Berkowsky, R., Winstead, V., & Anderson, W. (2017). *Designing technology training for older adults in continuing care retirement communities*. Boca Raton, FL: CRC Press.

Davidson, J.L., & Jensen, C. (2013). Participatory design with older adults: An analysis of creativity in the design of mobile healthcare applications. *Proceedings of the 9th ACM Conference on Creativity & Cognition* (pp. 114–123). New York: ACM. https://doi.org/10.1145/2466627.2466652.

Decker, M. (2008). Location privacy—An overview. *Proceedings of the 2008 7th International Conference on Mobile Business* (pp. 221–230). IEEE Computer Society Press. https://doi.org/10.1109/ICMB.2008.14.

Dwork, C. (2011). Differential privacy. In H.C.A. van Tilborg, & S. Jajodia (eds.), *Encyclopedia of Cryptography and Security* (second ed., pp. 338–340). Springer.

Farage, M.A., Miller, K.W., Ajayi, F., & Hutchins, D. (2012). Design principles to accommodate older adults. *Global Journal of Health Science*, *4*, 2–25. https://doi.org/10.5539/gjhs.v4n2p2.

Federal Register. (2017, January 19). Rules and regulations. *Federal Register, 82*(12), 7149-7274.

Franz, R.L., Baecker, R., & Truong, K.N. (2018). "I knew that, I was just testing you": Understanding older adults' impression management tactics during usability studies. *ACM Transactions on Accessible Computing (TACCESS)*, *11*(3), 1–23. https://doi.org/10.1145/3226115.

Future of Privacy Forum. (2017). *Understanding corporate data sharing decisions: Practices, challenges, and opportunities for sharing corporate data with researchers*. Available: https://fpf.org/2017/11/14/understanding-corporate-data-sharing-decisions-practices-challenges-and-opportunities-for-sharing-corporate-data-with-researchers/.

Future of Privacy Forum and Center for Democracy and Technology. (2012). *Best practice for mobile application developers*. Available: http://www.futureofprivacy.org/wp-content/uploads/Best-Practices-for-Mobile-App-Developers_Final.pdf.

Gatto, S.L., & Tak, S.H. (2008). Computer, internet, and e-mail use among older adults: Benefits and barriers. *Educational Gerontology, 34*, 800–811. https://doi.org/10.1080/03601270802243697.

Greene, D., & Shilton, K. (2017). Platform privacies: Governance, collaboration, and the different meanings of 'privacy' in iOS and android development. *New Media & Society*. https://doi.org/10.1177/1461444817702397.

Grindrod, K., Khan, H., Hengartner, U., Ong, S., Logan, A.G., Vogel, D., Gebotys, R., & Yang, J. (2018). Evaluating authentication options for mobile health applications in younger and older adults. *PLOS ONE, 13*(1), 1–16. https://doi.org/10.1371/journal.pone.0189048.

Hallinan, B., Brubaker, J.R., & Fiesler, C. (2019). Unexpected expectations: Public reaction to the Facebook emotional contagion study. *New Media & Society*. https://doi.org/10.1177/1461444819876944.

Harris, K.D. (2013). *Privacy on the go: Recommendations for the mobile ecosystem*. Sacramento, CA: California Department of Justice.

Heron, K.E., & Smyth, J.M. (2010). Ecological momentary interventions: Incorporating mobile technology into psychosocial and health behaviour treatments. *British Journal of Health Psychology*, *15*, 1–39. https://doi.org/10.1348/135910709X466063.

Joe, J., & Demiris, G. (2013). Older adults and mobile phones for health: A review. *Journal of Biomedical Informatics*, *46*, 947–954. https://doi.org/10.1016/j.jbi.2013.06.008.

Kang, H.G., Mahoney, D.F., Hoenig, H., Hirth, V.A., Bonato, P., Hajjar, I., Lipsitz, L.A., & Center for Integration of Medicine and Innovative Technology Working Group on Advanced Approaches to Physiologic Monitoring for the Aged. (2010). In situ monitoring of health in older adults: Technologies and issues. *Journal of the American Geriatrics Society, 58*, 1579–1586. https://doi.org/10.1111/j.1532-5415.2010.02959.x.

Kelley, P.G., Consolvo, S., Cranor, L.F., Jung, J., Sadeh, N., & Wetherall, D. (2012). A conundrum of permissions: Installing applications on an android smartphone. In J. Blyth, S. Dietrich, & L.J. Camp (Eds.), *Financial Cryptography and Data Security, Lecture Notes in Computer Science*, (pp. 68–79). Berlin, Heidelberg: Springer.

Kim, S.Y., Caine, E.D., Currier, G.W., Leibovici, A., & Ryan, J.M. (2001). Assessing the competence of persons with Alzheimer's disease in providing informed consent for participation in research. *The American Journal of Psychiatry, 158*, 712–717. https://doi.org/10.1176/appi.ajp.158.5.712.

Knowles, B., & Hanson, V.L. (2018). Older adults' deployment of "distrust." *ACM Transactions on Computer-Human Interaction (TOCHI), 25*(4), 1–25. https://doi.org/10.1145/3196490.

Koo, B.M., & Vizer, L.M. (2019). Mobile technology for cognitive assessment of older adults: A scoping review. *Innovation in Aging*, *3*(1), 1–14. https://doi.org/10.1093/geroni/igy038.

Kötteritzsch, A., & Weyers, B. (2016). Assistive technologies for older adults in urban areas: a literature review. *Cognitive Computation*, *8*, 299–317. https://doi.org/10.1007/s12559-015-9355-7.

Kowtko, M.A. (2014). Biometric authentication for older adults. *IEEE Long Island Systems, Applications and Technology (LISAT) Conference* (pp. 1–6).

Kuerbis, A., Mulliken, A., Muench, F., Moore, A.A., & Gardner, D. (2017). Older adults and mobile technology: Factors that enhance and inhibit utilization in the context of behavioral health. *Mental Health and Addiction Research*. *2*(2). https://doi.org/10.15761/MHAR.1000136.

Lindsay, S., Jackson, D., Schofield, G., & Olivier, P. (2012). Engaging older people using participatory design. *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 1199–1208). New York: ACM. https://doi.org/10.1145/2207676.2208570.

Lee, C., & Coughlin, J.F. (2015). PERSPECTIVE: Older adults' adoption of technology: an integrated approach to identifying determinants and barriers. *Journal of Product Innovation Management, 32,* 747–759. https://doi.org/10.1111/jpim.12176.

Lu, M.H., Lin, W., & Yueh, H.P. (2017). Development and evaluation of a cognitive training game for older people: A design-based approach. *Frontiers in Psychology*, *8* (Article No. 1837), 1–15. https://doi.org/10.3389/fpsyg.2017.01837.

Madden, Mary. (2012). *Privacy management on social media sites.* Washington, DC: Pew Internet Project. Available: http://www.pewinternet.org/2012/02/24/privacy-management-on-social-media-sites.

Madden, M., Gilman, M., Levy, K., & Marwick, A. (2017). Privacy, poverty, and big data: A matrix of vulnerabilities for poor Americans. *Washington University Law Review, 95*, 53–125.

Martin, D. (2007). Bureaucratizing ethics: Institutional review boards and participatory research. *ACME: An International E-Journal for Critical Geographies 6,* 319–328.

Martin, K., & Nissenbaum, H. (2016). Measuring privacy: An empirical test using context to expose confounding variables. *Columbia Science and Technology Law Review, 18,* 176–218.

Michener, W.K. (2015). Ten simple rules for creating a good data management plan. *PLoS Computational Biology, 11*(10), e1004525. https://doi.org/10.1371/journal.pcbi.1004525.

Narayanan, A., & Shmatikov, V. (2008). Robust de-anonymization of large sparse datasets. *Proceedings of the 2008 IEEE Symposium on Security and Privacy* (pp. 111–125). Oakland, CA: IEEE. https://doi.org/10.1109/SP.2008.33

Nath, R. K., Bajpai, R., & Thapliyal, H. (2018). IoT based indoor location detection system for smart home environment. *Proceedings of the 2018 IEEE International Conference on Consumer Electronics (ICCE)* (pp. 1–3). https://doi.org/10.1109/ICCE.2018.8326225.

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life.* Stanford, CA: Stanford Law Books.

Ohm, P. (2009). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review, 57,* 1701–1778.

Pandya, R.E. (2012). A framework for engaging diverse communities in citizen science in the U.S. *Frontiers in Ecology and the Environment, 10,* 314–317. https://doi.org/10.1890/120007.

Pew Internet Project. (2019). Mobile Fact Sheet. Available: https://www.pewresearch.org/internet/fact-sheet/mobile/.

Schreurs, K., Quan-Haase, A., & Martin, K. (2017). Problematizing the digital literacy paradox in the context of older adults' ICT use: Aging, media discourse, and self-determination. *Canadian Journal of Communication, 42*, 359–377. https://doi.org/10.22230/cjc.2017v42n2a3130.

Selinger, E., & Hartzog, W. (2016). Facebook's emotional contagion study and the ethical problem of co-opted identity in mediated environments where users lack control. *Research Ethics, 12,* 35–43. https://doi.org/10.1177/1747016115579531.

Serrano, K.J., Yu, M., Riley, W.T., Patel, V., Hughes, P., Marchesini, K., & Atienza, A.A. (2016). Willingness to exchange health information via mobile devices: findings from a population-based survey. *The Annals of Family Medicine, 14,* 34–40. https://doi.org/10.1370/afm.1888.

Shilton, K. (2009). Four billion little brothers?: Privacy, mobile phones, and ubiquitous data collection. *Communications of the ACM, 52,* 48–53. https://doi.org/10.1145/1592761.1592778.

Solove, D. J. (2010). *Understanding privacy.* Harvard University Press.

Sweeney, L. (2000). *Uniqueness of simple demographics in the U.S.* population (Technical Report No. LIDAP-WP4). Pittsburgh, PA: Carnegie Mellon University, School of Computer Science, Data Privacy Laboratory.

Turner, P., Turner, S., & Van De Walle, G. (2007). How older people account for their experiences with interactive technology. *Behaviour & Information Technology, 26*, 287–296. https://doi.org/10.1080/01449290601173499.

U.S. Department of Health and Human Services et al. (2016). *Use of electronic informed consent: Questions and answers. Guidance for institutional review boards, investigators, and sponsors*. Available: https://www.fda.gov/media/116850/download.

Valentino-DeVries, J., Singer, N., Keller, M.H., & Krolik, A. (2018, December 10). Your apps know where you were last night, and they're not keeping it secret. *The New York Times*. Available: https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

Vitak, J., Proferes, N., Shilton, K., & Ashktorab, Z. (2017). Ethics regulation in social computing research: Examining the role of Institutional Review Boards. *Journal of Empirical Research on Human Research Ethics, 12,* 372–382. https://doi.org/10.1177/1556264617725200

Vitak, J., Shilton, K., & Ashktorab, Z. (2016). Beyond the Belmont principles: Ethical challenges, practices, and beliefs in the online data research community. *Proceedings of the 19th ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW),* (pp. 941–953). New York: ACM. https://doi.org/10.1145/2818048.2820078.

Wagner, N., Hassanein, K., & Head, M. (2010). Computer use by older adults: A multi-disciplinary review. *Computers in Human Behavior, 26*, 870–882. https://doi.org/https://doi.org/10.1016/j.chb.2010.03.029.

Wandke, H., Sengpiel, M., & Sönksen, M. (2012). Myths about older people's use of information and communication technology. *Gerontology, 58*, 564–570.

Waycott, J., Vetere, F., Pedell, S., Morgans, A., Ozanne, E., & Kulik, L. (2016). Not for me: Older adults choosing not to participate in a social isolation intervention. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems,* (pp. 745–757). New York: ACM. https://doi.org/10.1145/2858036.2858458

Winstead, V., Anderson, W.A., Yost, E.A., Cotten, S.R., Warr, A., & Berkowsky, R.W. (2013). You can teach an old dog new tricks: A qualitative analysis of how residents of senior living communities may use the web to overcome spatial and social barriers. *Journal of Applied Gerontology, 32,* 540–560, 2013. https://doi.org/10.1177/0733464811431824.