Location Tracking with Transient IoT Devices: A Study of Users' Perceptions on the Privacy-Convenience Tradeoff

Emil Sohlberg, Joshua Soong, Clare Ulmer, Royce Yang, and Daniel Steinberg
The University of Chicago, Chicago, IL 60637

With the emergence of connectivity and wearable devices, users are becoming increasingly concerned with data privacy, especially related to Internet of Things (IoT) devices. While several studies have explored user sentiment in the domain of visory and auditory data, few have formally looked at users' perceptions of location data, which is both ubiquitous and powerful. In our study, we make use of Tile Bluetooth trackers for a 3-day pilot study in which we track participants' geo-coordinates. We visualize and present individualized location data during a semi-structured interview with the trackee. During the interview, we explore user opinions on how their own data should be processed, limited, or modified for sensitivity and personal privacy. We ultimately aim to gauge whether users believe that the convenience of IoT location tracking outweighs the associated privacy risks.

I. INTRODUCTION

In the modern age, location data has unequivocally become an integral component to many tasks we come across every day. Whether it is navigating to a restaurant with Google Maps, checking the Weather App, or booking an Uber, we can observe a myriad of benefits. However, the growing prevalence of location data collection and use has led to a simultaneous increase in concern for privacy and security. These concerns imply questions such as: *To what extent do users consider location tracking to be a convenience? Is that convenience worth the potential risk to privacy associated with location tracking? What types of settings would users like to be able to customize to protect their privacy? Is the same degree of protection necessary for different strengths of interpersonal relationships?*

Our study makes use of one of the most common location tracking devices: the Tile Bluetooth Tracker. The Tile is a small location tracking device that uses Bluetooth technology to connect to nearby smartphones and alerts its owner of its location through the Tile app. In our paper, we coin the term "transient IoT device" because by attaching the tile to an object, that object temporarily gains IoT-like abilities and the device user is able to track the location of that object. We exploit this feature by having participants carry the Tile around for the duration of the study. This allowed us to collect their location data.

Our pilot study consists of a 3-day tracking phase followed by a semi-structured interview where we ask the participant to view a visualization of their own data across the three days. Our visualizations included a scatter plot of different locations the user visited (using longitude and latitude as the axes) and a path plot of the path the user had traveled. Participants reflected on the accuracy of the data, their privacy concerns, how they would adjust (filter, delete, etc.) the data to ease their privacy concerns, and their opinions on the

balance of potential convenience and privacy risks of the location data collected from the Tile.

We found that while most participants agreed that there would be cases in which the Tile location data could be useful, they had concerns regarding its necessity. Some found the idea of being tracked to be scary and intrusive, indicating that they would like to be notified each time that their data was viewed or used by another individual. For privacy protection, participants suggested removing timestamps and only leaving location coordinates, restricting location sharing to temporary periods, and being able to remove specific data points.

Overall, the participants of our study came to a general consensus that IoT location tracking is not worth adopting. However, we do not make any strong conclusions, as our study faced several limitations. For one, because participation in our study was voluntary and self-selected, we ended up with a participant pool of 1 male and 7 female, all of which were students living in Hyde Park. Furthermore, due to the restriction of Tile location to only be accessible when the device is connected via Bluetooth to a smartphone that has the Tile app installed, we found that we were able to collect higher-quality data for individuals who spent more time in high-density areas like the library. Lastly, since we discussed potential conveniences of using Tile's location data verbally but the user did not actually experience those benefits, potential uses and benefits of Tile's location data could have been difficult for our participants to imagine.

II. RELATED WORK

Our study enters into the existing debate in the literature on what role transparency should play in how data is collected by IoT devices and mobile trackers. IoT devices in smart homes and mobile tracking are generally considered separately, but "thing"-oriented transient devices like Tile trackers [2] introduce questions of how the two fields intersect. Zachariah et al. [3] considered the new challenges posed by transient IoT devices on the practical level of internet gateways, noting the solution used by Tile and Fitbit [4] to "piggyback" their connective functions through nearby smartphones, similar to a system also suggested by Aloi et al. [5].

In the realm of privacy and security, there seems to have been little research specifically regarding the intersection between IoT and mobile devices offered by the transient devices like Tile. However, our work is related to research on issues of transparency in smart homes and the regulation of mobile device location data as well as work on the privacy considerations of internet-connected wearable devices.

IoT Transparency

One of the major debates around the Internet of Things involves finding how to optimally regulate access to the data that connected devices collect. A central goal of many IoT devices is to report information about the associated "things" they track. For devices intended for shared households or collaborative teams, sharing data across multiple users is a crucial convenience [6]. Sharing IoT data can also help increase a neighborhood's safety [7], or strengthen the bonds between parents and their adult children, as with the Messaging Kettle [8].

Too much transparency, on the other hand, can violate personal privacy. From a developmental health standpoint, full transparency could prove detrimental, as excessive surveillance can cause children to grow distrustful and antagonistic [9]. Additionally, though households are somewhat collectivist by nature, the United States is highly individualistic, which is reflected in the computer infrastructure that it exports. Young people are possibly directed towards independence by the prevalence of personal social media accounts, which could support an argument in favor of

lower transparency [10]. Furthermore, Ur et al. found that when given the tools to surveil, parents desire to use them to a far greater extent than children and teenagers are comfortable with [11]. IoT device owners in the context of a smart home are concerned about extending access to neighbors [7, 12], visiting families, babysitters, and, ironically, their children [12]. Our study seeks to build off these findings by understanding how this delicate management of access control extends from stationary IoT devices to intentionally portable ones.

Location Data Management

Transient IoT devices face similar privacy issues as those encountered in discussions around smartphone location tracking. These IoT devices tend to track location as an incidental function or as their primary function (e.g. Tile), although as part of the Internet of Things they differ from mobile phone tracking in their connection to a transient "thing" rather than an individual user.

Despite the sensitivity of the data, smartphone users already share their live location information with variable-sized groups of family, friends, and other acquaintances over popular apps like Apple's Find My Friends [13], the SnapMap function of Snapchat [14], and even dating apps [15]. Almuhimedi et al. found that users are often unaware of the extent to which applications collect their location data, but when presented with more transparent notices and usable tools for data management they tended to greatly restrict which apps could use that data [16]. Our own study explores a similar dynamic at work in transient IoT devices where social motives and convenience support transparency but users face lingering privacy concerns over excessive dissemination of sensitive location data.

III. METHODOLOGY

To capture as much data as possible and to put subjects into the context of a location tracking environment, we conducted a three-day study period followed by a semi-structured interview. We attempted to follow Charmaz's method [1] of conducting interviews until new themes stopped emerging, but, due to resource (i.e., Tile) and time constraints, we were only able to engage eight participants in our pilot study. Table 1 summarizes our participants and our interviews.

Number	Identifier	Major/Year	Gender	Interview Length
1	P01	Third Year	Female	42:07
2	P02	Second Year	Male	31:48
3	P03	Fourth Year	Female	20:02
4	P04	First Year	Female	42:57
5	P05	First Year	Female	28:01
6	P06	PhD Student	Female	39:15
7	P07	Second Year	Female	33:32
8	P08	Third Year	Female	29:26

Human Subjects and Ethics

We drafted but did not submit our ethics application to our institution's human subjects review board (IRB). Instead, our ethics applications were submitted to our instructors to ensure our study did not pose more than a minimal risk to our participants. Additionally, we obtained informed written and verbal consent from all participants. They consented to our collection of their location data and our audio recording of their

interviews. We ensured their data and interview recordings were always within our legal purview (i.e. we utilized a Booth School of Business computer cluster for location collection and SoundCloud, which explicitly leaves the legal rights of an audio bit with the uploader, for interview storage). Additionally, we scrubbed any metadata that could have been used to uniquely identify our participants.

Recruitment

We posted flyers around the University of Chicago campus and published Facebook posts in campus groups to attract participants. Student researchers utilized personal social media accounts to gain access to and publish recruitment materials online. Interested participants were directed to reach out to Joshua Soong, one of the student researchers, via email. Upon successful screening, we reached out to subjects to set up a meeting time to obtain consent and to give them a Tile tracker. We asked that they carry their Tile on their person at all times to ensure the accuracy of collected location data.

Study Period

At 8 A.M. the day after we gave subjects a Tile tracker, we began collecting their location data. We collected data every 15 minutes for the next three days. We felt that a 15 minute time interval was long enough to avoid collecting too many "side-by-side" data points but short enough to avoid missing important location data. Due to the nature of our recruitment, many of our subjects were students, and 15 minutes was a roughly appropriate amount of time to account for travel time in between classes.

In order to collect data, we built a Python script using PyTile, a Python API for Tile Bluetooth tracking, and ran it on the Mercury computing cluster at the Booth School of Business. Because the Slurm job scheduler had a duration restriction of scripts to be less than 48 hours, we interpolated our data collection through multiple process instances.

The script worked by pinging each of the Tiles every 15 minutes for a duration of 72 hours. The script then recorded the last location that the Tile was seen as a JSON file containing information on the Tile ID, timestamp, and geo-coordinates.

It should also be noted that, while our sample size was small, we made an effort to stagger study periods. Rather than running one study of eight subjects, we ran two rounds of four subjects. We staggered the rounds' start and end dates by one day in an attempt to capture as much location diversity as possible. Since we hypothesized subjects would be more active during the weekend, we made an active attempt to include Saturday and Sunday in the time frame for both rounds of participants.

Interview Design

Upon the conclusion of the three-day study period, we set up semi-structured interviews with all subjects. We chose to conduct in-person interviews at the John Crerar Library as we felt meeting participants face-to-face would enable us to ask probing questions and better understand subjects' thought processes during the think aloud portion of the interview. Interviews typically lasted 33 minutes, with the shortest being 20 minutes and the longest being 43 minutes.

We designed our interviews with three primary goals in mind: a) exploring the tradeoff between privacy and security, b) understanding location tracking from a trackee's perspective and a hypothetical tracker's point of view, where trackee refers to a person whose location data is being viewed by another person while tracker refers to the person who is able to view another's location data, and c) soliciting feedback on a interface paper prototype our team built. A complete script of our interview questions can be found in the appendix. Generally, our interviewers followed

the interview script unless a subject posed an interesting thought that warranted further investigation. When this occurred, interviewers asked probing questions designed to get them to elaborate on their thought process.

To start we asked four high-level questions about the privacy-security questions. We intentionally put these questions first because we did not want to bias their answers with the results of the three-day trial period. We then utilized their collected location data to understand trackee and tracker perspectives on privacy and security. Since they had their location data tracked during the study period, we attempted to put them first into the context of the trackee. We did this by aggregating their location data into several maps that we presented to them. Maps were created by plugging the gathered location data into the gmplot Python library and generating both scatterplots and path maps, which were viewable within Google Maps sections of .html files. The scatterplots showed points in different locations of varying darkness, representing the duration of time or number of times spent in that location. The path maps connected all of the gathered data points and connected them with blue lines in order to show the route a participant traveled that day.

Finally, we asked the participants to give feedback on the permissions and privacy settings on a paper prototype of a location tracking settings interface. This paper prototype, which was created using Justinmind, a free app mockup software, has been attached in the appendix. The paper prototype served two purposes. First, it enabled us to validate or refine our hypothesis about which privacy permissions and settings users would want to have access to. Next, although it was truly a paper prototype (not a phone app), it also provided a more real world context and something tangible that subjects could interact with.

Finally, interviews were independently coded by both the primary interviewer and a secondary researcher. Creating this codebook enabled us to verify our themes and results amongst each other.

IV. RESULTS

Our research question asked whether, given their desired settings, participants found IoT location tracking to be a convenience worth the associated privacy risk. This question can be broken down into three sub-questions: first, do participants consider IoT location tracking a convenience? Second, is the convenience associated with IoT location tracking worth the potential risk to privacy associated with IoT location tracking as-is (i.e., as is currently possible or available with existing products and settings)? And finally, if the answer to the previous question is no, does the existence of the participant's desired settings change this answer? In other words, are personalized settings enough to make IoT location tracking a convenience worth the privacy risk?

The presentation of our results addresses these three questions in turn. Broadly speaking, we found that many participants view IoT location tracking as something that could theoretically be useful or convenient but that is in actuality not particularly applicable to their lives. Our participants expressed dissatisfaction with existing models of tracking (e.g., constant live location tracking). They highlighted how existing tracking models can lead to altered behavior, strained social relationships, and concern over how corporations use their data. Our participants theorized that certain limits or restrictions would make IoT location tracking more palatable to them in a home environment. They also highlighted uses for IoT location tracking that did not involve sharing but focused instead on analysis of one's own behavior.

Convenience and Uses of Tracking

Our interview asked participants to think about what benefits might be associated with using Tile to share locations with close relations including

friends, roommates, or family members. Participants' ideas about ways to use Tile for IoT location sharing between close relations generally fell into three categories: convenience, safety, and entertainment/social. However, many participants specified that these were *possible* ways to use IoT location tracking and sharing but not ways that they would actually incorporate into their own lives.

Convenience

Nearly every participant gave a scenario in which using Tile for IoT location tracking amongst close relations could be convenient, and almost all of these scenarios centered around meeting up with people more easily. Participants said that IoT location sharing would be helpful in contexts when you are supposed to meet a friend but they are not there (P8) or when you want to see which of your friends are in the area so that you can run into them (P4). One participant (P7) also mentioned that IoT location tracking could help solve a problem where one of your friends is lost. Two participants (P4, P7) mentioned that IoT location tracking could be convenient for parents who are "paranoid" or who want to be able to check in on their kids when they feel it's necessary. P7 specifically stated that while her mother tracks her, she believes her mother doesn't always monitor her location, but rather uses it as a way to have "peace of mind."

Safety

All but one participant (P8) mentioned using IoT location tracking for safety purposes. Three participants (P1, P4, and P5) mentioned tracking as a way to ensure the safety of small children or teenagers. P1 mentioned using tracking when in a "caretaker role" for elderly relatives, children, or those who wander off, and P8 specified that parents might use location tracking to ensure that their kids get to school safely if they are navigating through a city. Other participants (P2, P5, P6, P7) mentioned using IoT location tracking to ensure the safety of their friends or to have friends help with the participant's own safety. Participants mentioned a variety of scenarios: both tracking friends who are inebriated, have impaired decision-making skills (P2), or are meeting up with people they met online (P7), and being tracked themselves when going on a date with a stranger (P6), walking at night as a woman (P7), and going on a hike (P6). P1 also mentioned IoT location tracking as being particularly useful in situations where there is an emergency and/or a person cannot make a phone call—in this case, a tracking device like a Tile could be used as a "panic button." Finally, two participants (P1, P4) mentioned tracking pets as a way to keep them safe.

Entertainment / Social Reasons

Three participants (P4, P6, P8) mentioned tracking as a "fun" activity or a way to facilitate entertainment or social relationships. P4 mentioned that tracking could be a way to see if there are friends around you when on vacation. P6 mentioned sharing road trips as a way to use IoT location tracking amongst friends for entertainment. Finally, P8 mentioned that tracking could be used for "fun" purposes such as seeing one's own data when traveling or being aware of one's own behavioral patterns. Unlike P4 and P6, P8 spoke about entertainment purposes as ways that tracking could be interesting for oneself, not in sharing contexts.

Concerns and Use in Own Life

All but two participants indicated that they either had concerns about potential uses of IoT location tracking or would not find it necessary to use in their own life, or both. P1, P7, and P8 all explicitly stated that they found IoT location tracking, broadly speaking, to be unnecessary to use in their own lives. P7 stated that there were no real advantages to sharing locations with friends. P8 stated that she didn't see any purpose in tracking her own family and that the existing functions of tracking weren't sufficient to make tracking roommates worthwhile.

P2, P5, and P6 all identified issues they had with location tracking. P2 said that he would only use tracking if forced. P5 and P6 both said that they had concerns about IoT location tracking thatbeing used for abusive or manipulative reasons amongst close relations. P5 specified that she didn't approve of parents using location data about their children as information with which to discipline their children.

Obstacles to Adopting IoT Location Tracking with Current Model

Evidently, most of our participants did not feel that, under current models of IoT location tracking and sharing, the services or conveniences provided by this tracking were worth adopting. In this section, we identify a number of qualms participants had with existing models of tracking. These can be grouped into four broad categories: constant tracking, altered behavior, social relationships, and companies' data collection.

Constant Tracking

Five participants (P1, P3, P4, P5, P8) mentioned constant tracking. P1, P3, and P4 all found constant tracking "scary" or "invasive." P4 mentioned that constant tracking could also be harmful to safety—for instance, it could allow someone to know when you're not home and then break into your house. P5 and P8 did not describe constant tracking explicitly but said that they thought current location was the more useful information (P5) and that they thought that they would only use live tracking during short time intervals (P8).

Altered Behavior

Participants had a fairly wide range of views about whether tracking would alter their behavior. P3 and P7 said that because they would only share their location with people that they were very close to, they didn't think that they would alter their behavior when being tracked. P4 and P6 said that they wouldn't alter their behavior if they were given the option to turn the tracker on and off at specific times, but P6 said that if the tracker were always on, she would change her behavior. P7 and P8 mentioned awareness of tracking as being important to their attitudes—P7 said that her increased awareness of phone location tracking made her uncomfortable, and P8 said that whether or not her behavior would be altered would depend on how obvious the tracking is. For P8, the Tile being "cute" mitigated how intrusive tracking felt. P1 and P5 said, generally speaking, that people act differently when they know they are being watched. Finally, P2 mentioned that knowledge of tracking creates a "chilling effect." He felt that he would be more cautious about where he went and might even feel that he couldn't go certain places or maintain his normal behavior. P3 mentioned a positive element of changed behavior as a result of being tracked: it might encourage someone to be more active. In sum, most participants mentioned altered behavior (largely in a negative context, with the exception of P3) as a potential result of IoT location tracking.

Social Relationships

Participants mentioned a number of scenarios in which IoT location tracking could present a problem or could be undesirable in the context of social relationships. P2 specified that IoT location tracking was only ever acceptable in a context where both parties had explicitly given consent. Similarly, P3 said that she would not be comfortable tracking someone who didn't know they were being tracked. P2, P4, P7, and P8 all mentioned specific social scenarios related to IoT location tracking that they found undesirable. P2 mentioned wanting to see data on his personal device only rather than on a public (e.g., available to all members of a home) screen in order to ensure that no one else would "accidentally" see his data or data shared with him. P4 asserted that location data "isn't other people's business"; similarly, P7 stated that she would be suspicious if someone really wanted to know her location

information. Finally, P8 stated that she would not want her parents to be able to see her location when going out.

Companies' Data Collection

Four participants (P1, P2, P3, P7) brought up non-individual use of IoT location data. P1 and P7 both said that companies' access to location data was more concerning to them than access by close relations. P2 and P7 both mentioned advertisements and personalization, though P2 said that these were very concerning and could be "used against you" while P7 founds ads "not that big of a problem" because she was not personally influenced by them. P7 also mentioned leaks as concerning. She thought that tech companies mostly seem secure, but she would be uncomfortable (though not concerned for her safety) with data leaks involving her information.

Desired Limits and Modifications on IoT Location Tracking

In addition to eliciting participant opinions about potential uses of IoT location tracking and associated concerns, we asked participants to think about what kind of limits they would want on IoT location tracking. The goal of this part of the interview was both to highlight the elements of IoT location tracking participants found most undesirable (and thus wanted to limit) and also to gauge whether or not these limits would make IoT location tracking sufficiently acceptable for participants to use in their own lives. In this section, we outline those limits and modifications, which fall into three categories: notification of data collection, on/off functionality, and types of data being collected and shared. Following that, we discuss how participants had different ideas about IoT location data when they thought about keeping data for themselves as opposed to sharing it.

Notification of Data Collection

Three participants (P1, P5, P6) mentioned that they would want to be aware of when other people were looking at their location data. P1 and P6 mentioned that they would want to be notified when their location was being accessed, but they did not specify how they wanted this notification to be structured. In contrast, P5 said that she would want people to "ask before seeing data," which implies that a request to see data would have to be approved by her. What P5 described would likely resemble a blocking notification for the user—that is, a notification that they would have to respond to or make a decision in response to before any further action or data sharing could take place. It is unclear whether P1 and P6 would want control over whether or not to share location data when they received a notification, or if they believe that awareness of data sharing would be sufficient.

On/Off Functionality

Four participants (P2, P5, P6, P8) discussed wanting an option to turn IoT location tracking or its associated features on and off. P5 and P6 discussed this limit in general terms. P8 mentioned specific ways that on/off options might work: turning tracking in general on and off (starting and ending a "tracking session" manually), turning "certain features" (unspecified) on and off, and turning certain measures of activity like times sitting or standing on and off. P2 said that he would want to be able to set a geographical boundary outside of which he could no longer be tracked.

Types of Data Being Collected and Shared

Two participants (P1, P4) mentioned that they would only want other people to be able to see their live location. They would not want other people to have access to location history. P1 specified that she was against sharing location history because she would not want her long-term behavioral patterns to be trackable or reconstructable. P4 said that she thought information about past locations was "pointless" and an "unnecessary privacy invasion." She said that friends didn't need to know location history

and that live location was more useful to share for the purposes she was thinking of. She did say, however, that location history could be useful for oneself.

Two participants (P3, P8) said that they would restrict location sharing to certain times of day or to temporary periods.

Several participants talked about wanting limits on sharing metadata about their location. P3 and P6 said that they would not want their location data to include timestamps. P2 also said that he would not want data about frequency of visits to certain locations to be shared. This echoes concerns raised by P1 and P4 about location history and behavioral patterns as sensitive data.

Four participants (P2, P4, P6, P8) said that they would want the option to remove certain data points. P4 and P8 specified how they would evaluate which points to remove: P4 said that she would like the option to remove "sketchy" points, and P8 said that she would like the option to remove data that she wouldn't want a specific person to see if that person would otherwise have access to her location data overall.

Individual participants had a few other suggestions for limitations on data or ways to modify data. We have only included ideas that came up in two or more participant interviews.

V. DISCUSSION

There are a few takeaways from the results we observed. The first is a possible answer to our research question: "Given their desired settings, do users see IoT location tracking as a convenience worth the privacy risk?" Since the majority of participants mentioned tracking as not being worth adopting, the answer must be no, but this should be unpacked further. As far as what privacy risk there is to tracking, participants did come up with some negative consequences that could arise, such as corporate data leaks or criminals knowing when a home is absent and free to burglarize. However, these privacy issues were not explicitly stated as reasons why tracking would not be adopted. The corporate data leak issue was one that we expected might be mentioned by participants, as they could have suggested setting some limits on what kind of data corporations would be able to collect, use, or store, but the absence of this suggestion could mean that the issue overall ranks relatively low on participants' minds. Though participants recognized that the tracking could be useful socially, such as for locating inebriated or lost friends, the privacy angle of making this data available to friends or acquaintances was either not addressed, or explained away in that only close relations would ever be given access. Overall, it seems privacy issues are noncritical, or adequately resolved by "desired settings". To explain why users were not enthused about tracking, privacy issues were listed only as one group among several others, relating to both the general unease that comes with tracking, as well as the service seeming just not that useful in the first place. So while the answer to our research question is no, it is not necessarily the privacy risks that are preventing tracking from being desirable, but rather other properties inherent to tracking. Even when discussing possibilities for their desired settings, the participants said it was unlikely that they would use tracking in the future.

There are also a number of avenues for future research. Since participants seemed unenthusiastic, a new tracking prototype could be designed to target some of the exact use cases that they listed, such as tracking inebriated friends, or providing more security walking home at night. Since these uses are situational, running the study over a longer period of time would make sense, giving more opportunities for the prototype to be used. Privacy could still be incorporated, maybe through an app permissions angle, such as if the

prototype was always tracking location data even when not in use. However, privacy could just as easily be removed from this hypothetical study, since participants were not all that concerned, and a future study could focus more on what would actually make tracking useful instead.

There were some significant limitations to our study. The first had to do with how the Tile Bluetooth trackers function. Having only Bluetooth capabilities, they are accurate only in proximity to phones with the Tile app installed. This resulted in a serious confound where the visualized data given to participants during the interview phase was of varying levels of accuracy. In the future, we would want to use a more precise tracking mechanism, or possibly pull data from Google Maps' API. Another data-related confound was the fact that two out of our eight participants started their three-day tracking period a day earlier than the others. Though our intention was for all participants to be tracked over a Thursday-Friday-Saturday period, to capture both weekday and weekend kinds of activity, two participants were tracked over a Wednesday-Thursday-Friday period instead. Another limitation had to do with our small sample size, and limited diversity among participants, though as a pilot study this was to be expected. We had only eight participants, all of whom were University of Chicago students, and seven out of eight of whom were female. These shared characteristics lead our findings to have limited external validity.

VI. CONCLUSION

While our study presents a framework of privacy concerns and user-desired settings regarding tracking location data, we are unable to make any definitive conclusions due to the lack of external validity from our under-represented participant pool and potentially biased presentation of data during the interviews that made it easier to perceive the risks than the benefits. Nevertheless, our interviews from the pilot study lead to an interesting array of IoT location data-related privacy concerns, desired settings, and questions open for exploration. While we do not recommend using the Tile for continued research on IoT location privacy due to its device-specific limitations, we do believe that our privacy framework, constructed specifically for location data, is invaluable towards further understanding the cost-benefit tradeoff of convenience and privacy for IoT devices using location information.

VII. ACKNOWLEDGEMENTS

We thank Blase Ur and Weijia He for their instruction, as well as for their help advising us and discussing with us this pilot study as it has evolved through its various stages. We also thank our anonymous participants for taking the time to carry the Tiles and for participating in our post-tracking interviews.

This work was supported by the University of Chicago.

VIII. REFERENCES

[1] Charmaz, K. Constructing Grounded Theory, second ed. SAGE Publications Ltd, 2014.

[2] Tile Inc. Tile. http://thetileapp.com.

[3] Zachariah, T., Klugman, N., Campbell, B., Adkins, J., Jackson, N., and Prabal, D. The Internet of Things Has a Gateway Problem. In *Proceedings of the 16th International Workshop on Mobile Computing Systems and Application* (Santa Fe, NM, 2015), pp. 27-32.

[4] Fitbit Inc. Fitbit. https://www.fitbit.com/home.

[5]. Aloi, G. Caliciuri, G. Fortino, R. Gravina, P. Pace, W. Russo, and C. Savaglio. Enabling IoT interoperability through opportunistic

smartphone-based mobile gateways. In *Journal of Network and Computer Applications, Volume 81* (2017), pp. 74-84.

[6] Lekakis, G., Basagalar, Y., and Keleher, P. Don't Trust Your Roommate or Access Control and Replication Protocols in "Home" Environments. In Proc. HotStorage (2012).

[7] Brush, A. B., Jung, J., Mahajan, R., and Martinez, F. Digital Neighborhood Watch: Investigating the Sharing of Camera Data Amongst Neighbors. In Proc. CSCW (2013).

[8] Brereton, M., Soro, A., Vaisutis, K., and Roe, P. The Messaging Kettle: Prototyping Connections over a Distance between Adult Children and Older Parents. In CHI (2015).

[9] Schechter, S. The User IS the Enemy, and (S)he Keeps Reaching for that Bright Shiny Power Button! In Proc. HUPS (2013).

[10] Stobert, E., and Biddle, R. Authentication in the Home. In Proc. HUPS (2013).

[11] Blase Ur, Jaeyeon Jung, Stuart Schechter. Intruders versus Intrusiveness: Teens' and Parents' Perspectives on Home-Entryway Surveillance. In Proceedings of UbiComp 2014.

[12] He, W., Golla, M., Padhi, R., Ofek, J., Dürmuth, M., Fernandes, E., and Ur, B. Rethinking Access Control and Authentication for the Home Internet of Things (IoT). In Proc. 27th USENIX Security Symposium (USENIX Security 18) 2018.

[13] Jons, B. PSafe. "The Pros and Cons of Find My Friends." http://www.psafe.com/en/blog/pros-cons-find-friends/

[14] Evans, G. Complex Media. "Snapchat's New Snapmap feature is going to Ruin Your Life." https://www.complex.com/life/2017/06/snapchat-snap-map-feature

[15] Hoang, N. P., Asano, Y., and Yoshikawa, M. Your neighbors are my spies: Location and other privacy concerns in dating apps. 2016 18th International Conference on Advanced Communication Technology (ICACT)

[16] Almuhimedi, H., Schaub, F., Sadeh, N., Adjerid, I., Acquisti, A., Gluck, J., Cranor, L. F., and Agarwal, Y. Your Location has been Shared 5,398 Times!: A Field Study on Mobile App Privacy Nudging. In Proceedings of CHI 2016.

VIV. APPENDIX

A. Location Tracking Code

https://raw.githubusercontent.com/royce1998/Files/master/tile.py

B. Visualization Generation Code (external file)

imagegen.py

Code used to generate HTML visualizations of tracking data

Usage: python3 imagegen.py uuid starttimestamp endtimestamp

Filename: imagegen.py

C. Ethics Application (external file)

NB: This ethics application was submitted before our project was altered based on feedback from Blase. Updated versions of some parts of the ethics application (such as the survey questions) have been included in the appendix below. Our project was re-designed to decrease the risks associated with the project we wrote about in the ethics application; as such, we believe that the ethics of this project have been sufficiently taken in to account in the process of conducting our research.

D. Interview Script

Thank you for taking the time to participate in our study. Our goal is to better understand privacy and security in the context of the Internet of Things, the home environment, and location tracking. As the three-day study period has concluded, we will now ask you to answer questions about your experience during the study.

Background Information

- Have you used Tiles before for keeping track of items or sharing your location?
- Have you used phone apps like Snapchat or Find My Friends to share location information with friends in the past?
    - If yes, when did you first start using the app(s)? How regularly do you use it, and what are your location sharing settings.
    - If no, have you heard of the services before? What do you think about them?
- Describe your social media usage in general.
    - Which social media do you use?
    - How often do you post on those?

General

- In the context of privacy and convenience, what do you think of location tracking between individuals who are friends, roommates, or have other close relationship?

As the Trackee

In these next questions, we're going to ask you to answer from the perspective of someone being tracked.

- What benefits do you see in using Tiles to share your location with friends?
- How do you see sharing this data as potentially being useful?
- Do you think you might change behavior due to your location information being shared?
- What privacy concerns, if any, do you have?
- Suppose you are designing a mobile app to aggregate the data you just collected about your location data. What types of preferences and settings would you like to have available?
- Look at the your location data that was collected during the three day study period. As you think about it, feel free to just state any and all reactions you have aloud.
    - Is there anything that surprises you? Why?

    - Would you add any restrictions to when, how, or where your Tile is tracking you? Why?
    - Do these visualizations seem accurate or inaccurate?
    - Do you like or dislike certain visualizations? Why?
- If this location data was instead being shared with a close relation, are there any permissions or restrictions that you would like placed on your data? Why?
    - Would you remove or modify any of your data?

As the Tracker

Now suppose that instead of using this app yourself, you are tracking a close relation who is carrying the Tile.

- What types of settings and preferences would you like to have available to you?
    - Please justify and explain your settings. Why do these differ from if you were using the app to track yourself?
    - Paper prototyping is where one designs the possible layouts of an interface. Please paper prototype this app <give paper and pen>.

Interface Paper Prototype

- Now, look at this paper prototype. Please focus on the settings and preferences. [the following questions are asked about each screen of the interface prototype]
    - Do you agree with the available preferences and settings?
    - What else would you like to see?
    - What else would you like removed?
    - Is there anything you don't understand or that you think is unclear?

General Questions

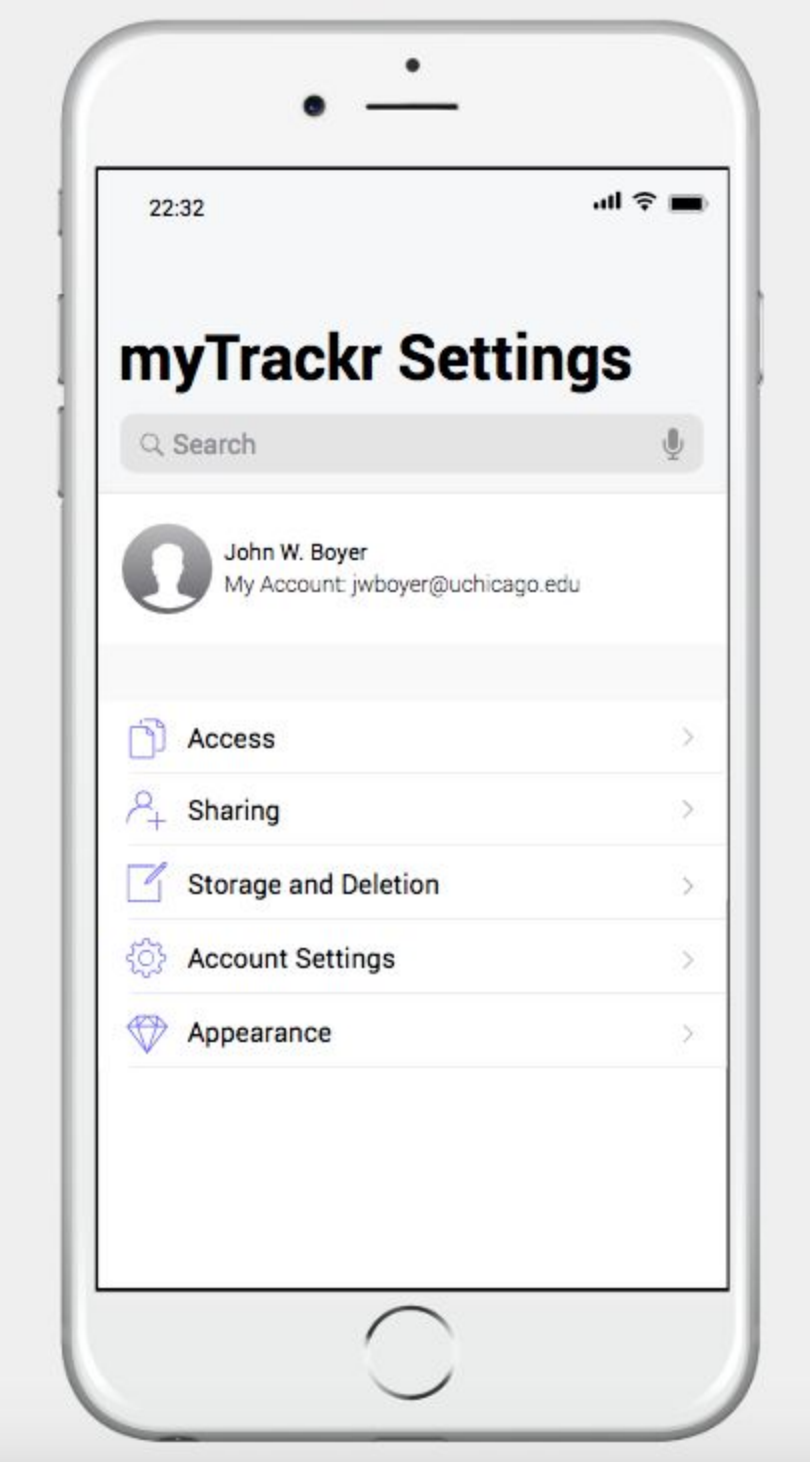
- How would you access this type of data in a home context?
- What kinds of modification of location data would you like to be able to make?
- How would you go about sharing your location data with others in your home given the ability to set preferences in the ways we've explored during this interview?

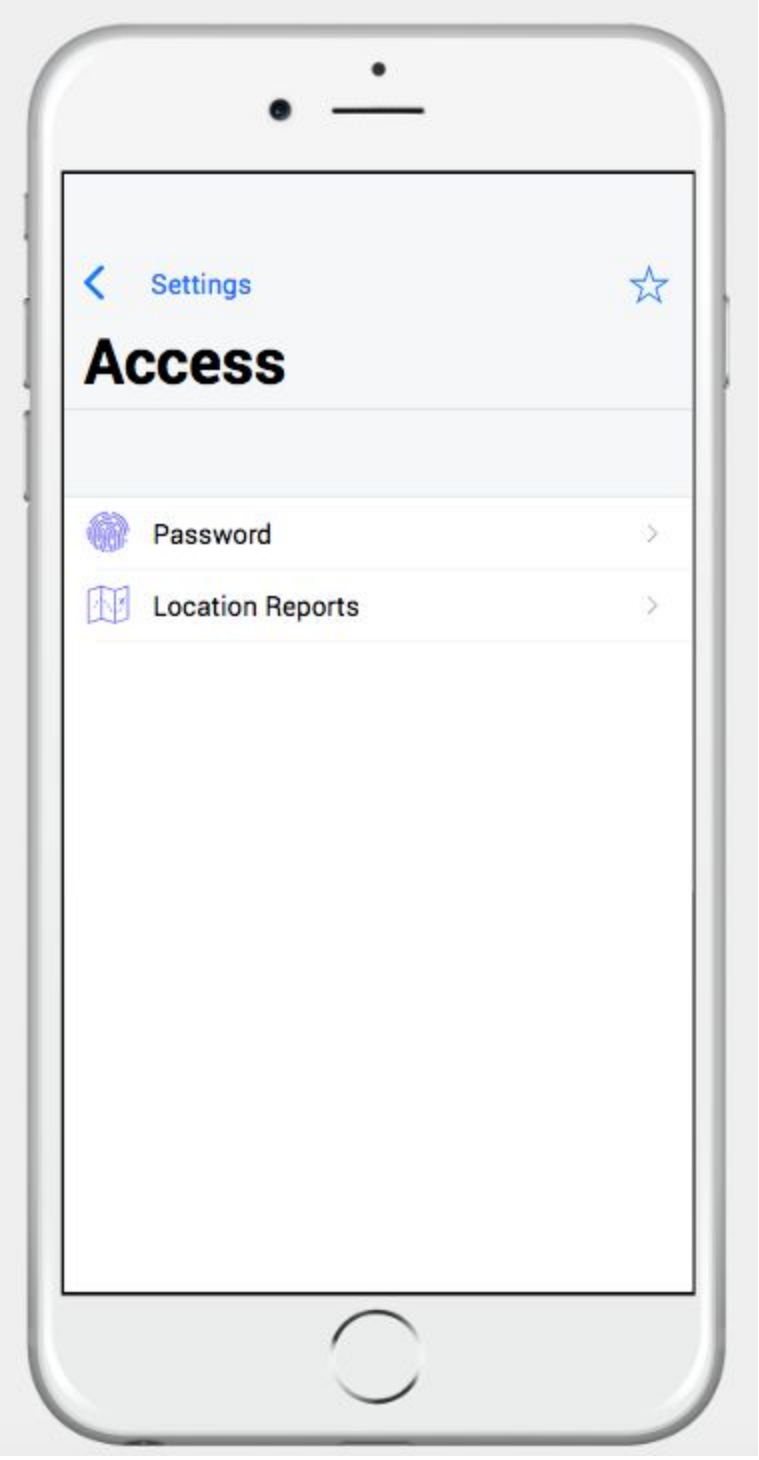
Demographics

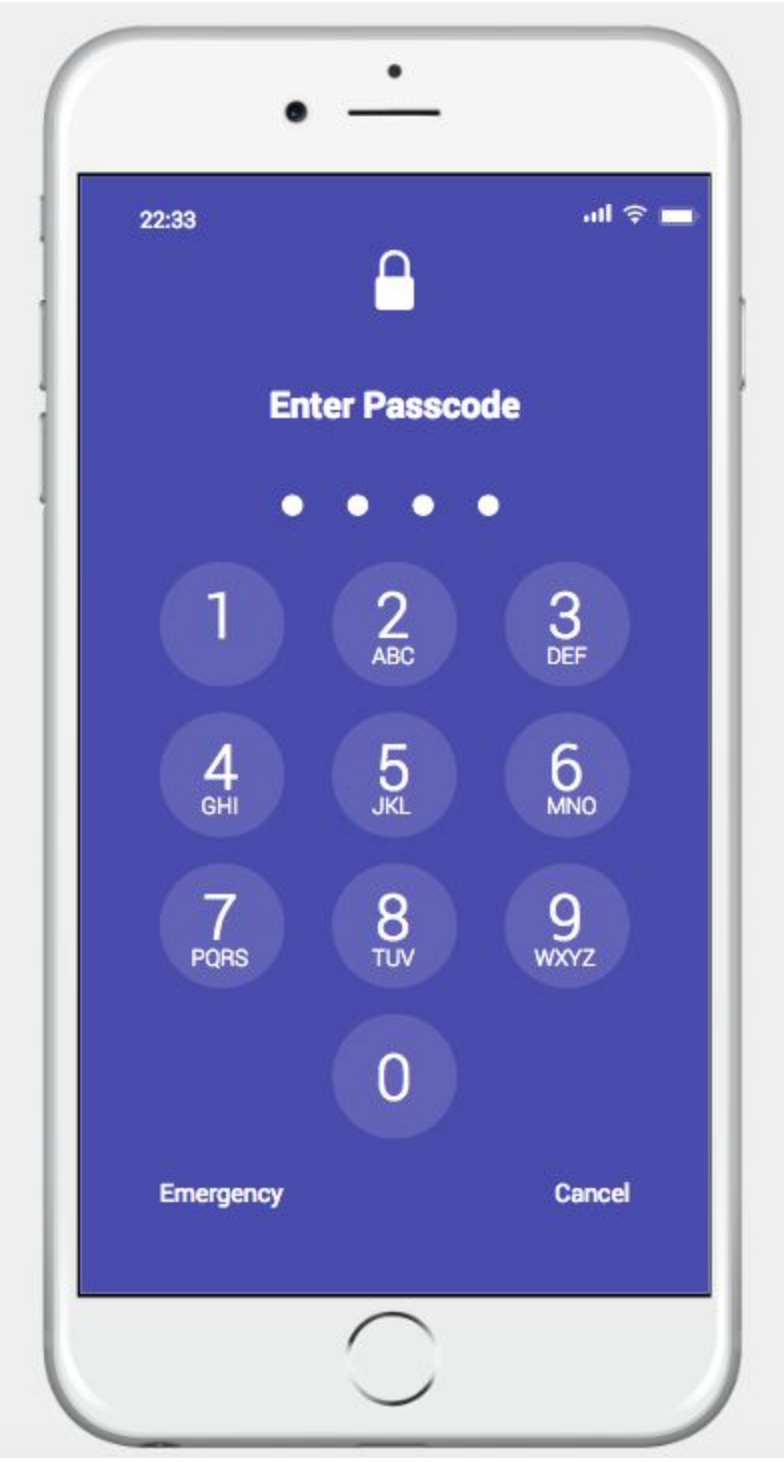
Please feel free to decline to answer any of these questions.

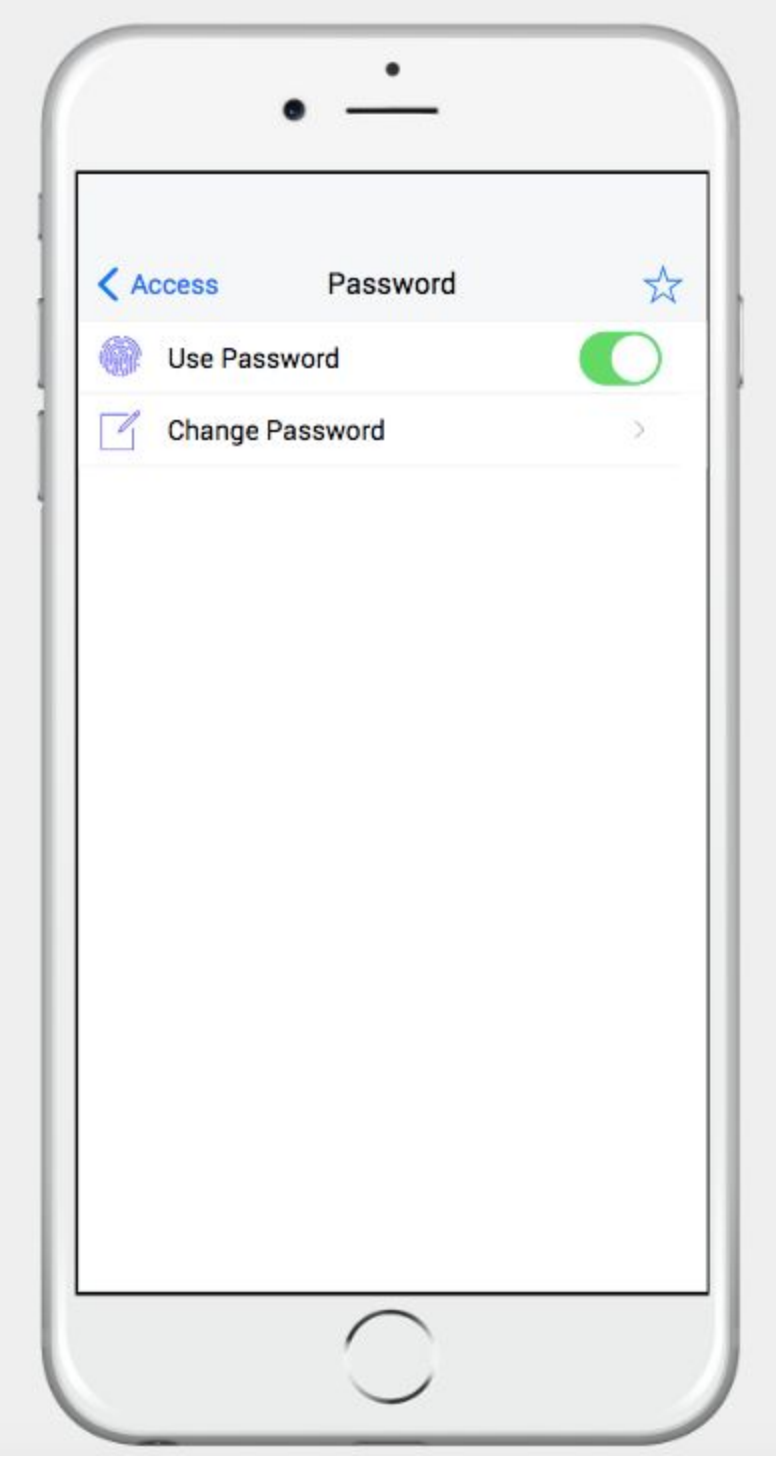
- What is your gender?
- What is your ethnicity?
- What grade are you in?
- How old are you?
- What is your major?

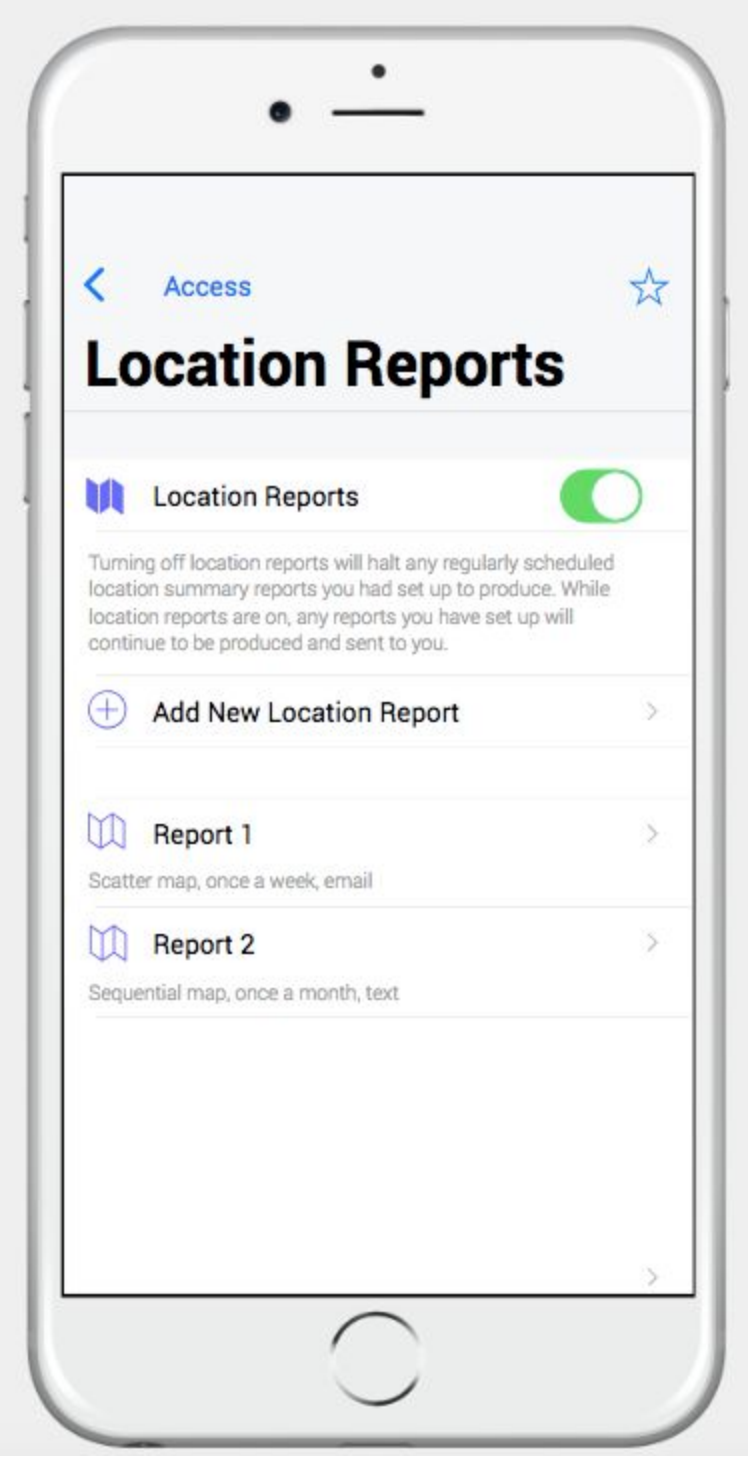
E. Interface Prototypes

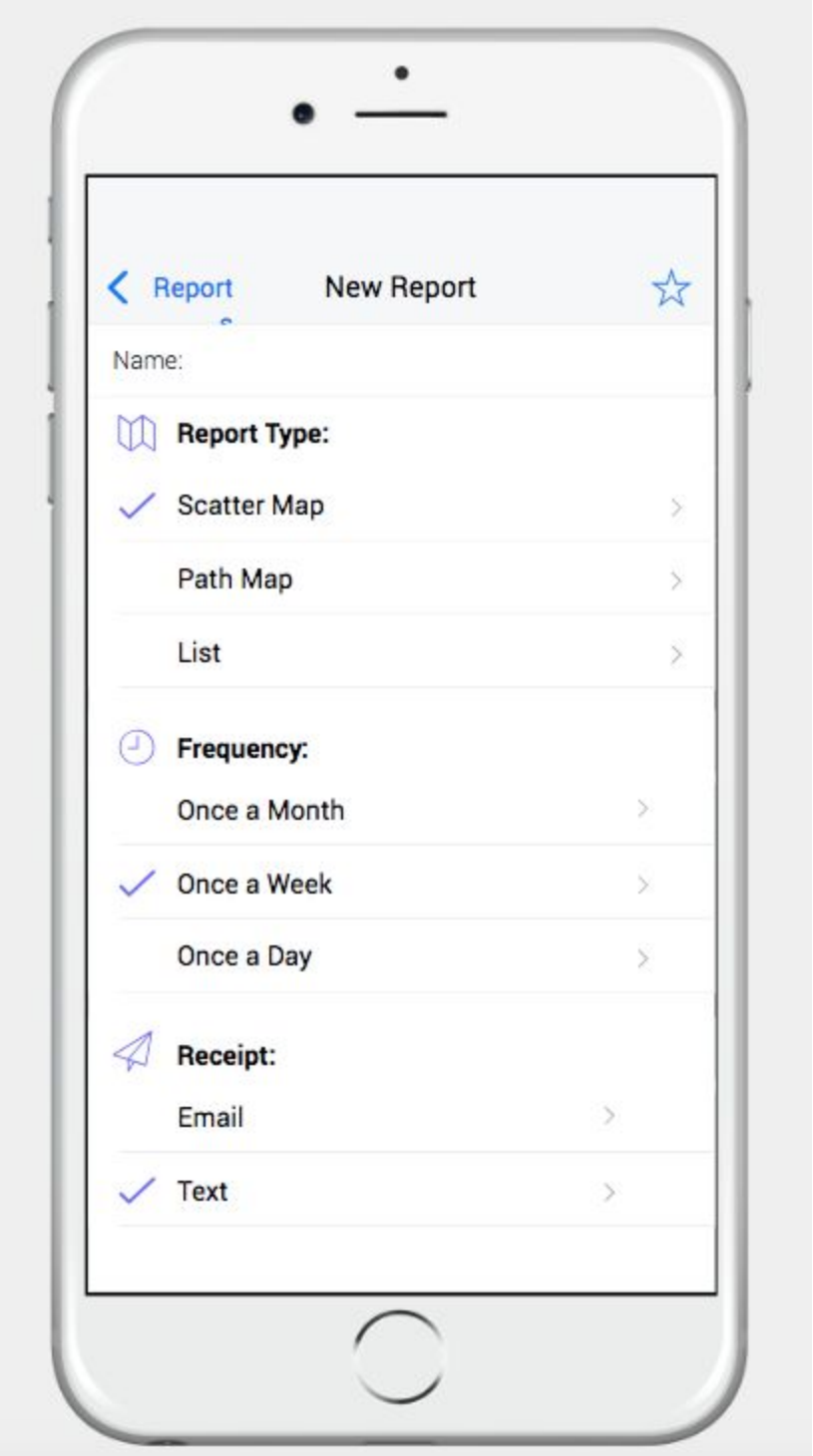

22:32
myTrackr Settings
Search
John W. Boyer
My Account: jwboyer@uchicago.edu
Access
Sharing
Storage and Deletion
Account Settings
Appearance

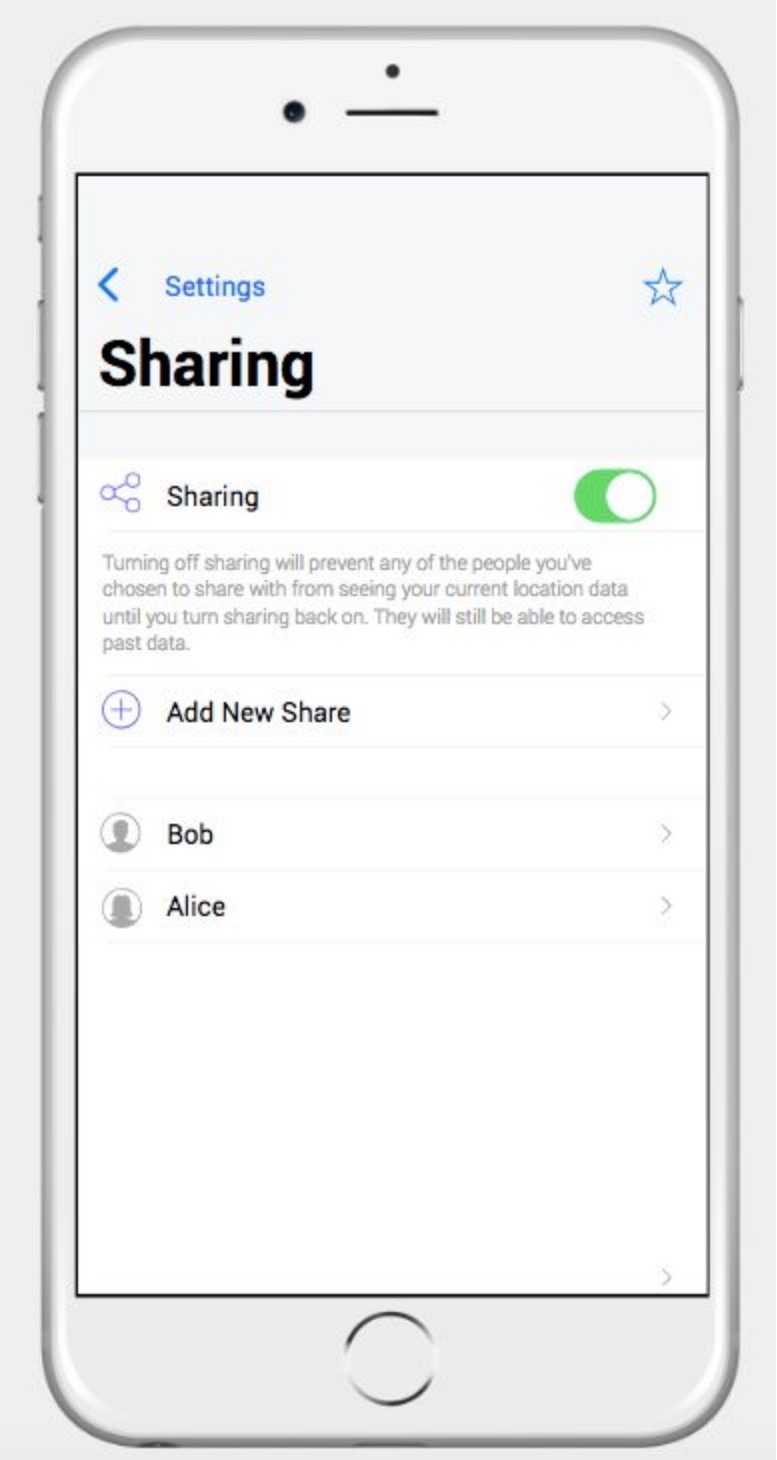

Settings
Access
Password
Location Reports

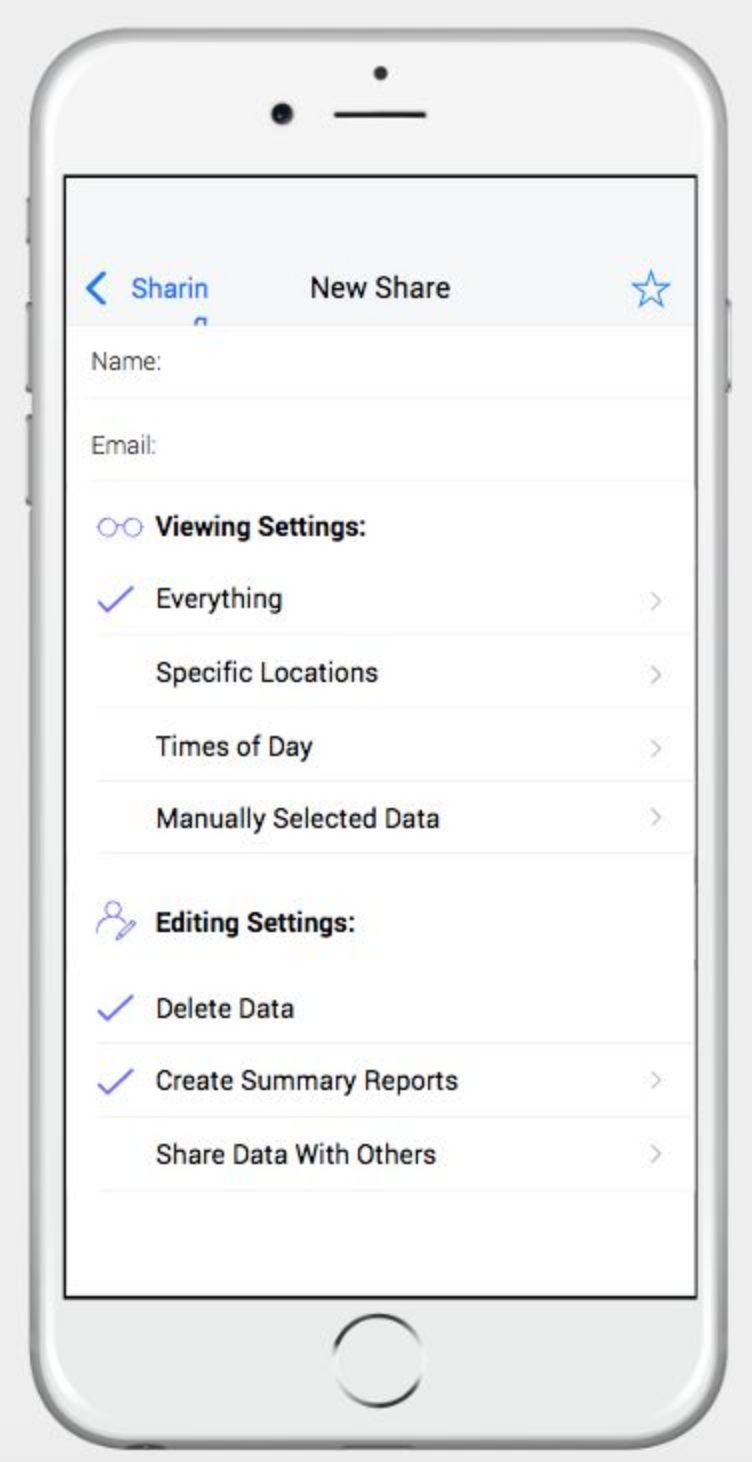

22:33
Enter Passcode
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
0
Emergency
Cancel

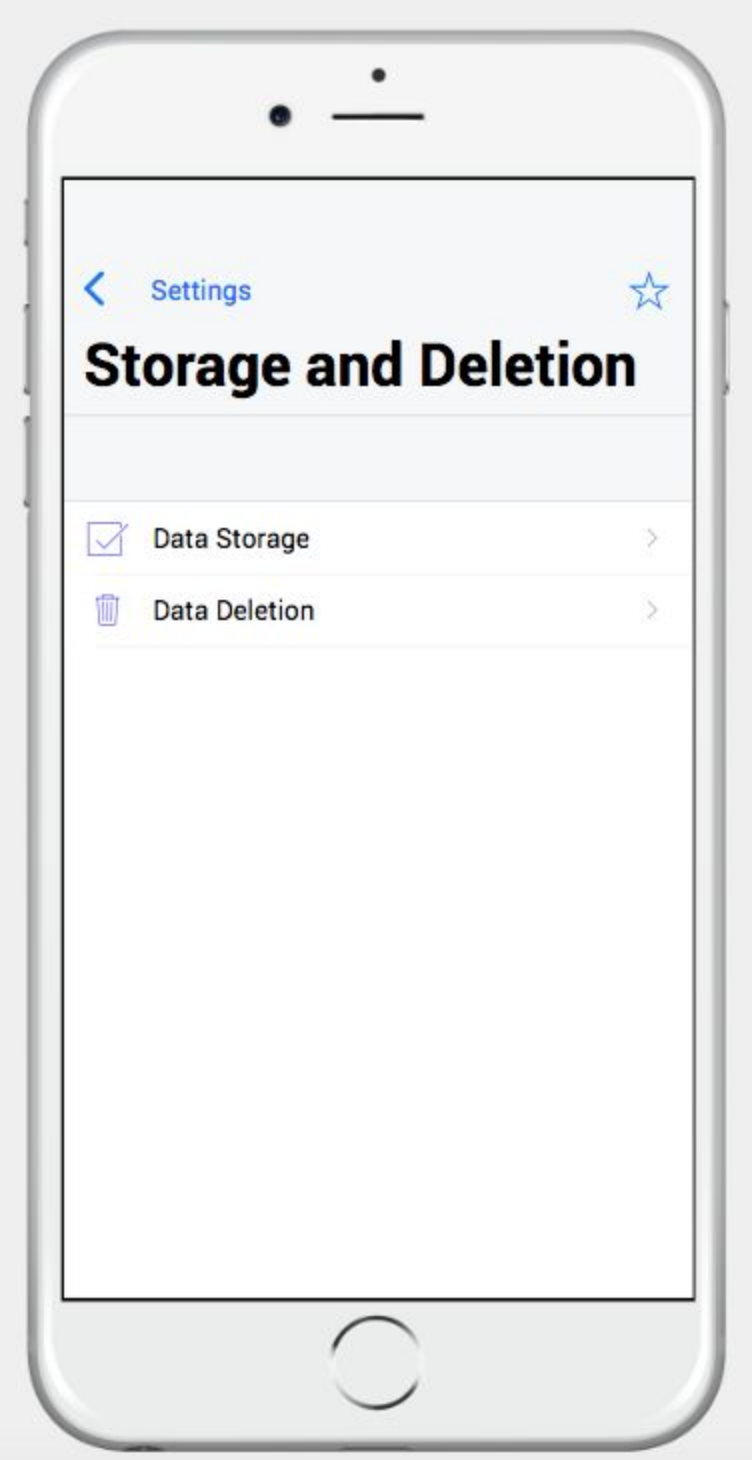

Access
Password
Use Password
Change Password

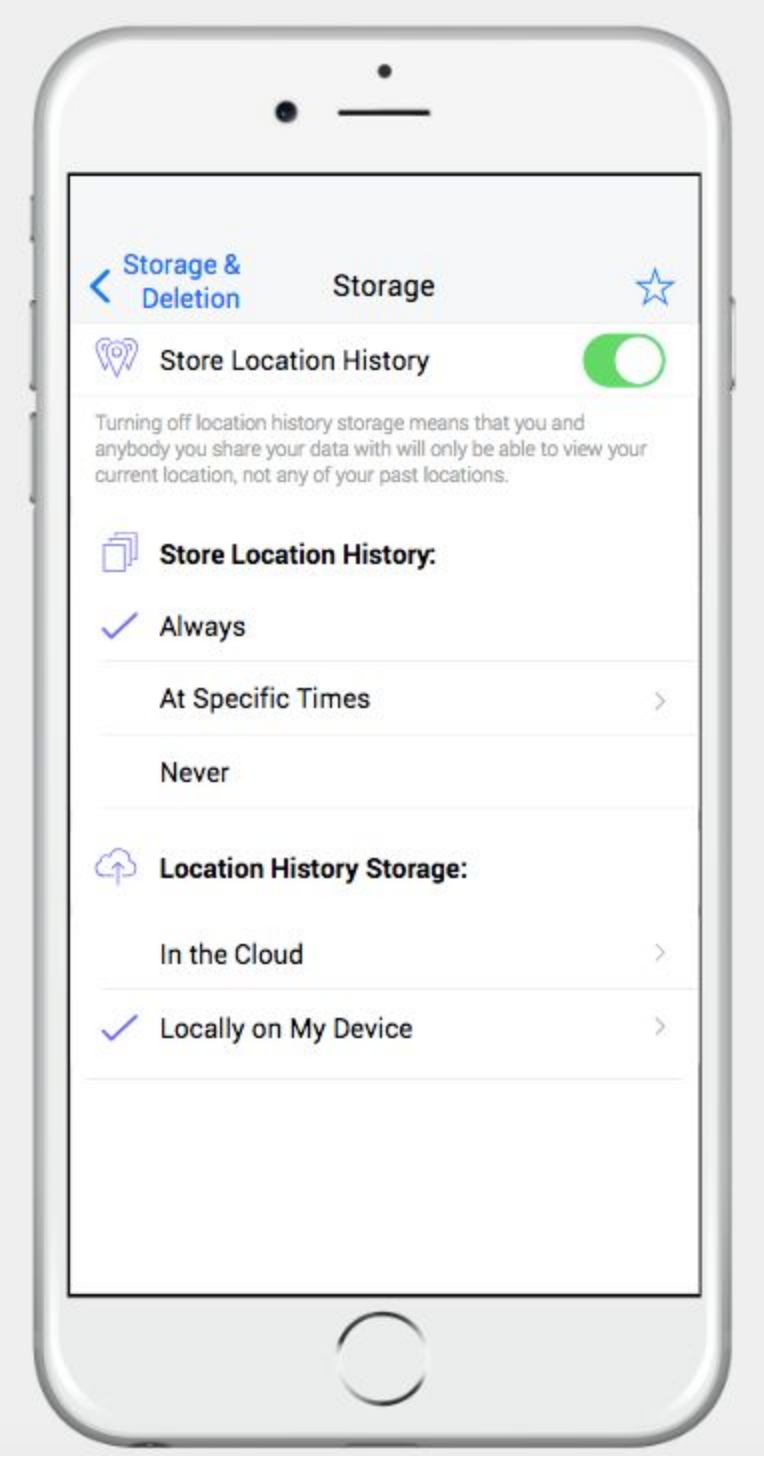

Access
Location Reports
Location Reports
Turning off location reports will halt any regularly scheduled location summary reports you had set up to produce. While location reports are on, any reports you have set up will continue to be produced and sent to you.
Add New Location Report
Report 1
Scatter map, once a week, email
Report 2
Sequential map, once a month, text

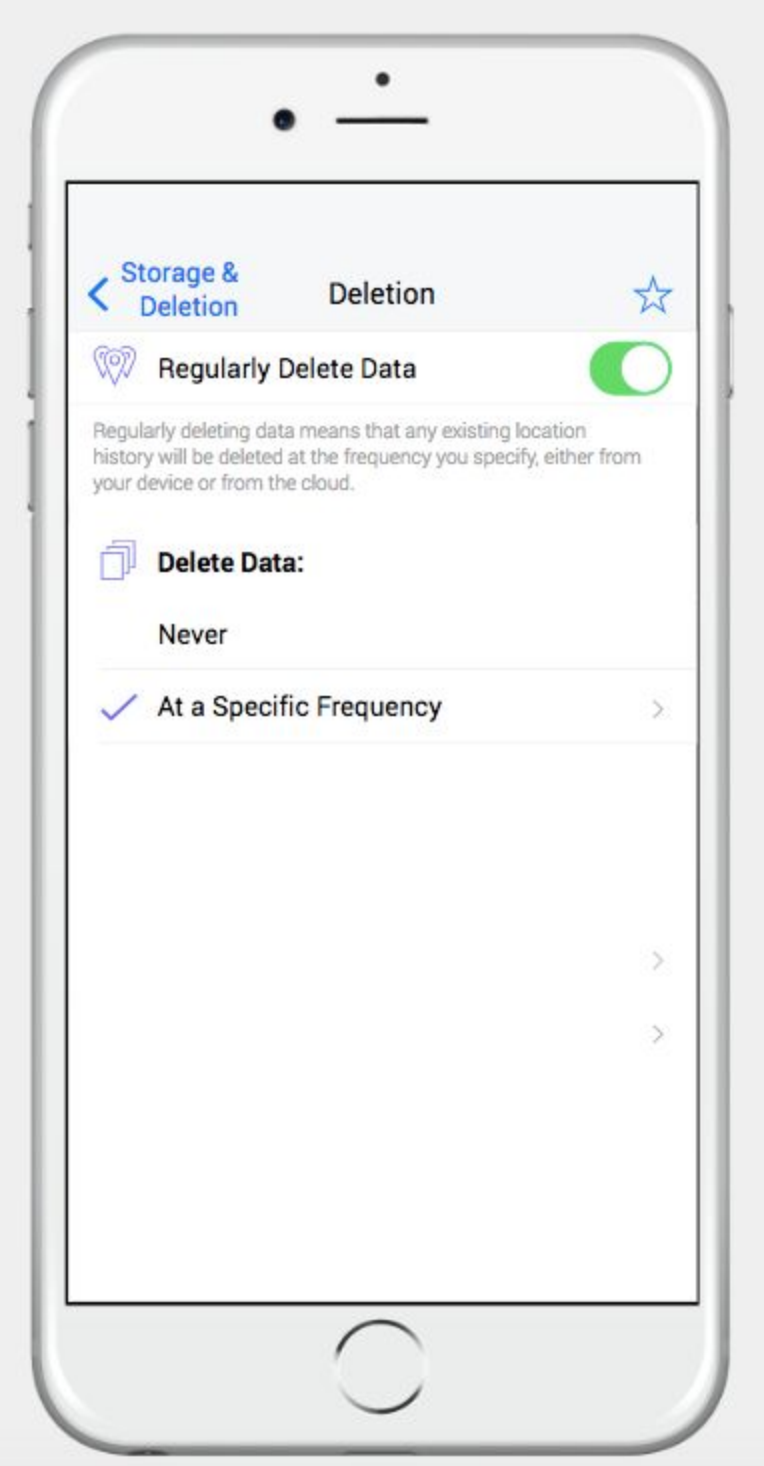

Report
New Report
Name:
Report Type:
Scatter Map
Path Map
List
Frequency:
Once a Month
Once a Week
Once a Day
Receipt:
Email
Text


Settings
Sharing
Sharing
Turning off sharing will prevent any of the people you've chosen to share with from seeing your current location data until you turn sharing back on. They will still be able to access past data.
Add New Share
Bob
Alice


Sharin
New Share
Name:
Email:
Viewing Settings:
Everything
Specific Locations
Times of Day
Manually Selected Data
Editing Settings:
Delete Data
Create Summary Reports
Share Data With Others


Settings
Storage and Deletion
Data Storage
Data Deletion


Storage & Deletion
Storage
Store Location History
Turning off location history storage means that you and anybody you share your data with will only be able to view your current location, not any of your past locations.
Store Location History:
Always
At Specific Times
Never
Location History Storage:
In the Cloud
Locally on My Device


Storage & Deletion
Deletion
Regularly Delete Data
Regularly deleting data means that any existing location history will be deleted at the frequency you specify, either from your device or from the cloud.
Delete Data:
Never
At a Specific Frequency