Considering smartphones: User attitudes towards privacy and trust in location-aware applications

Caitlin D. Cottrill, Lecturer
School of Geosciences, Department of Geography & Environment
University of Aberdeen
St Mary's Building, Elphinstone Road
Aberdeen, UK AB24 3UF
c.cottrill@abdn.ac.uk
Tel: +44 (0)1224 273694

Word Count: 5,115 + 6 Figures + 2 Tables = 7,115

Abstract:
The rapid adoption of smartphones and the location-sensing applications for which they provide a platform has provided scope for efficient and dispersed collection of location information that may be beneficial to the field of transportation. The quality and comprehensiveness of such data, however, depend in large part on the attitudes of users towards these applications, their trust in the application developers and data users, and their practices relative to these applications in the context of their personal use. In this paper, we initiate an exploration of some of these issues using a stated preference and self-reported behavior survey of US-based smartphone users in order to generate an understanding of underlying issues that may impact the quality and quantity of data collected through these technologies.
According to the Pew Research Center’s Internet & American Life Project’s summer 2012 report, roughly 45% of US adults (or about 108 million people) over the age of 17 currently own a smartphone (1). A separate 2012 Pew report found that of those Americans with smartphones, roughly 75% use some sort of location-based service (2). This growing ubiquity of smartphones and attendant location-enabled apps portends likely benefits for the transportation industry. Increasing research on the use of GPS-enabled smartphones for the dissemination of travel surveys, combined with the massive quantities of location and travel behavior data currently collected by such apps as Foursquare and Google Maps, brings a new era for the collection and mining of detailed, extensive data sets that can greatly assist the transportation professional. In addition, targeted transportation information such as bus arrival times and safe bicycle routes may be provided to users via use of specialized apps that draw upon the availability of location sensors.

One concern, however, lies in questions related to privacy and trust in the context of app use, and how questions or concerns about them may impact user interaction. Given that one of the expected benefits of these technologies is the ability to collect, share and use detailed, accurate location and mobility data over time, trust concerns that cause participants to reduce their sharing of data may limit the ability of planners, engineers, and others to realize the full potential benefits. Attendant issues, such as attitudes towards privacy and willingness to share and disseminate information, need also to be addressed as part of this research, as this will influence what we may expect from collected data.

In this study, we will examine emerging trends of location-enabled smartphone app adoption, looking, in particular, at attitudes towards potential concerns (i.e., privacy and trust) and how these may impact, or be reflected in, patterns of behavior. Existing data sources on app adoption will be leveraged and expanded into a survey to examine in more detail how current users of smartphones make choices related to location-enabled app use and their attitudes regarding these app benefits and concerns. Findings will be used to propose methods by which identified concerns may be adequately addressed by app developers and data users.

We will first review existing research on smartphone adoption rates and dissemination of location-based applications. Next, we will examine the types of data that may commonly be gathered through use of these applications, and how they are treated within the public and private sectors regarding regulations on sharing and/or selling. Following this discussion, we will report the findings of a pilot survey of 120 U.S.-based smartphone users on their use of location-sensing apps, and their concerns and attitudes regarding trust and use of these technologies. Results from this initial survey will be examined, and areas of needed future research identified to ensure that user concerns are addressed in relation to location based smartphone applications such that the data gathered through use of these apps may itself be trusted. It is anticipated that this study will provide an initial analysis of areas of concern to be examined as we move towards the use of ubiquitous technologies for support of transport planning and projects.
calling. In addition to their built-in functions, smartphones run myriad free and paid applications, turning the once single-minded cellphone into a mobile personal computer (3). The rapid adoption rate of smartphones has relied in large part on the widespread implementation of the underlying infrastructure necessary for their effective operation, including global positioning systems (GPS), wireless network access points for Wi-Fi, and 3 and 4G (third and fourth generation) networks. In addition, the importance afforded to the smartphone has also been reflected in growing investments made in research and development of these resources in the areas of government, private corporations, and public and private institutions (4, 5).

In addition to investments being made in technological and infrastructure improvements in support of smartphone deployment, many resources are also being invested in development for smartphones. The market for mobile applications ("apps", or small programs designed to run on mobile computing platforms) has been growing rapidly, with estimates recently showing the Apple App Store with roughly 775,000 and the Google Play/Android market with approximately 800,000 apps (6) available for smartphones and tablet computers. The purchase and/or download of these apps has also been growing rapidly – as of May 2013, Apple was reporting 50 million downloads and Google Play 48 million (7).

It is evident from these figures that the use of smartphones and attendant apps has become fairly commonplace over the last several years. It should be noted, however, that differences are still evident in the sociodemographics of persons who use smartphones, in the types of applications they use, and in how they treat their personal information. For example, according to findings from the Pew Research Center (2013), younger, more educated, urban males tend to be more likely to use smartphones, though growth has been seen across most demographic sectors as smartphones have become more common, and as more developers enter the app market.

Such rapid adoption and dissemination, however, initiates concerns over the data that such apps collect, and with whom it is shared. As part of the Wall Street Journal's "What They Know" series, they evaluated a set of 101 popular applications (50 each for Android and iPhone, along with the WSJ's app for each) to determine what information was being collected, and with whom it was shared. While they tested a range of data types (including username and password; contacts, age and gender; location; phone ID; and phone number), the findings regarding location data sharing were particularly revealing. For the iPhone, the study found that 26 of the 50 apps shared location data with third parties, while an additional six shared this data with the app developer (8). For the Android, 21 apps shared location data with third parties, and an additional four with the app developer (8). Such findings have a number of implications for the transport and mobility sectors.

First, it provides an indication that a large number of applications are collecting and sharing location data, which may signal the potential for public transportation agencies to partner with application developers to access detailed, useful data on a sample of the population. At the same time, however, it indicates the potential lack of regulation overseeing this market sector, which may reduce the willingness of public agencies to tap into this data source. Such implications suggest the need to better understand the landscape of the use of location-aware applications, and how user adoption of and behavior regarding them may impact the quality of data collected, as well as the manner in which partnerships are made. The following section will present the preliminary results of a small survey undertaken to begin to address some of these questions.

SURVEY OVERVIEW AND FINDINGS

Overview
In conducting the research related above, it was noted that there is little extant information available on trust in the context of location-sensing smartphone applications, and how this may impact or influence a user’s behavior regarding these applications. Because the manner in which a consumer interacts with an application may impact on the value of data gathered through these applications, and due to outstanding questions regarding data quality in the context of provenance, we determined to conduct a short stated preference survey to assess attitudes towards privacy in the mobile environment, if and how these attitudes may influence a consumer’s use of specific types of location-sensing apps, and if users have been proactive in maintaining or adjusting privacy settings in consideration of their concerns. We generally hypothesize that users will indicate that they have privacy concerns related to their use of location-sensing applications, but that this will not necessarily be reflected in their use of these applications in a way that would impact the quality of the location data from a planning point of view. An initial survey was developed and tested by six pilot participants. Pilot responses led to the elimination of two questions, and additional definitions and examples given for a number of terms used in the survey (such as geo-fencing) in order to ensure clarity and comprehension.

For purposes of this survey, we recruited 120 participants using the Amazon Mechanical Turk (MTurk) marketplace. Each respondent was paid US$0.50 for completing an 18-item survey lasting roughly 9 minutes. The survey was hosted on the website SurveyMonkey, and all participants were asked to confirm that they reside in the United States, are 18 years of age or older, and own a smartphone. We acknowledge that the use of MTurk for selecting our sample will create a biased sample population; however, as this is intended to provide an initial assessment of the landscape regarding smartphones and location privacy, we felt that the trade-off between obtaining a geographically dispersed sample of persons who are not affiliated with the researcher was more appropriate than obtaining a general convenience sample. The use of Mechanical Turk has been supported by researchers such as Paolacci, et al (2010), who report that, despite some differences with the overall US population, MTurk respondent results are comparable to other Internet samples or samples obtained from college campuses; Buhrmester, et al (2011), who found that MTurk samples tend to be more demographically representative than traditional convenience samples or college-based sample sets; and Berinsky, et al (2012), who found that MTurk respondents are generally representative of the US population, though potentially younger and slightly more liberal ideologically. If we estimate a US population of adults over the age of 18 as roughly 231,195,000, and accept that approximately 56% own a smartphone (1), this leaves our estimated population of interest as 129,469,200. A sample size of 120 provides us with a confidence level of 95% with a margin of error of +/- 8.95. While rough estimates subject to bias from demographic discrepancies, we feel that this sample is adequate for an initial assessment of attitudes towards privacy in the context of location-sensing applications. Figure 1 below provides a map of the geographic locations of respondents.
Though heavily weighted towards the northern and eastern portions of the United States, patterns and centers of the US population are reasonably well reflected in the location of respondents. It is not possible to calculate the survey response rate, as we cannot track the number of persons who were eligible to participate in the survey and who also viewed the assignment. Of the 128 persons who consented to the requirements and began the survey, 120 persons (set as the upper limit) finished the instrument, for a completion rate of 93.75%. Respondents were asked a number of questions regarding their use of location-aware applications along with a number of demographic questions.

Findings

General Results

120 persons completed the survey. Demographic characteristics of respondents are shown in Table 1. While the response population skews slightly younger, wealthier, and more highly educated than the general US population, it is roughly reflective of patterns of smartphone ownership in the United States, as reported in (1). Participants reported using a variety of different smartphone types, with most reporting using Android (56%) or iPhones (41%).
<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Total</th>
<th>% total</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Age</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18-20</td>
<td>16</td>
<td>13.3%</td>
</tr>
<tr>
<td>21-29</td>
<td>56</td>
<td>46.7%</td>
</tr>
<tr>
<td>30-39</td>
<td>29</td>
<td>24.2%</td>
</tr>
<tr>
<td>40-49</td>
<td>13</td>
<td>10.8%</td>
</tr>
<tr>
<td>50-65</td>
<td>6</td>
<td>5.0%</td>
</tr>
<tr>
<td>65+</td>
<td>0</td>
<td>0.0%</td>
</tr>
<tr>
<td><strong>Gender</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Male</td>
<td>66</td>
<td>55.0%</td>
</tr>
<tr>
<td>Female</td>
<td>54</td>
<td>45.0%</td>
</tr>
<tr>
<td><strong>Employment Status</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employed, working 1-34 hours per week</td>
<td>28</td>
<td>23.3%</td>
</tr>
<tr>
<td>Employed, working 35 hours or more per week</td>
<td>59</td>
<td>49.2%</td>
</tr>
<tr>
<td>Not employed, looking for work</td>
<td>19</td>
<td>15.8%</td>
</tr>
<tr>
<td>Not employed, not looking for work</td>
<td>13</td>
<td>10.8%</td>
</tr>
<tr>
<td>Retired</td>
<td>0</td>
<td>0.0%</td>
</tr>
<tr>
<td>Disabled, not able to work</td>
<td>1</td>
<td>0.8%</td>
</tr>
<tr>
<td><strong>Currently enrolled as student</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes, studying full time</td>
<td>25</td>
<td>20.8%</td>
</tr>
<tr>
<td>Yes, studying part-time</td>
<td>7</td>
<td>5.8%</td>
</tr>
<tr>
<td>Not currently a student</td>
<td>88</td>
<td>73.3%</td>
</tr>
<tr>
<td><strong>Education level</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Less than a high school degree</td>
<td>0</td>
<td>0.0%</td>
</tr>
<tr>
<td>High school graduate</td>
<td>11</td>
<td>9.2%</td>
</tr>
<tr>
<td>Some college</td>
<td>43</td>
<td>35.8%</td>
</tr>
<tr>
<td>Associates degree</td>
<td>12</td>
<td>10.0%</td>
</tr>
<tr>
<td>Bachelor's degree</td>
<td>42</td>
<td>35.0%</td>
</tr>
<tr>
<td>Master's degree</td>
<td>9</td>
<td>7.5%</td>
</tr>
<tr>
<td>Professional degree</td>
<td>3</td>
<td>2.5%</td>
</tr>
<tr>
<td>Doctorate degree</td>
<td>0</td>
<td>0.0%</td>
</tr>
<tr>
<td><strong>Household Income</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No response</td>
<td>6</td>
<td>5.0%</td>
</tr>
<tr>
<td>$0-$24,000</td>
<td>20</td>
<td>16.7%</td>
</tr>
<tr>
<td>$25,000-$49,999</td>
<td>39</td>
<td>32.5%</td>
</tr>
<tr>
<td>$50,000-$74,999</td>
<td>25</td>
<td>20.8%</td>
</tr>
<tr>
<td>$75,000-$99,999</td>
<td>14</td>
<td>11.7%</td>
</tr>
<tr>
<td>$100,000-$124,999</td>
<td>7</td>
<td>5.8%</td>
</tr>
<tr>
<td>$125,000-$149,999</td>
<td>4</td>
<td>3.3%</td>
</tr>
<tr>
<td>$150,000-$174,999</td>
<td>1</td>
<td>0.8%</td>
</tr>
<tr>
<td>$175,000-$199,999</td>
<td>2</td>
<td>1.7%</td>
</tr>
<tr>
<td>$200,000+</td>
<td>2</td>
<td>1.7%</td>
</tr>
</tbody>
</table>

Participants were next asked the following question:

- Do you use any of the following types of location-sensing apps or services on your smartphone?
  - Navigation (such as Google Maps, Mapquest, Waze)
  - Public transport information (such as CTA Bus Tracker, TfL Journey Planner, AllSubway)
  - Other transport information/services (such as GetTaxi, mytaxi, BikeMap)
Generally, this question was designed to understand the overall use of location-aware applications in order to obtain a ground-level understanding of how acceptable or applicable location-sensing apps are to smartphone users. It was found that survey respondents use an average of five of the location-aware application types surveyed ($SD=1.9$ applications), with no statistically significant difference found between usage by gender. Results of this question, broken down by smartphone type, are shown in Table 2.

### TABLE 2 Location Application Use by Phone Type

<table>
<thead>
<tr>
<th>Phone Type</th>
<th>Navigation</th>
<th>Transit Information</th>
<th>Other Transport Information</th>
<th>Place Annotation</th>
<th>Social Networking</th>
<th>Travel</th>
<th>Recommendations</th>
<th>Geo-Fencing</th>
<th>Health &amp; Fitness</th>
<th>Mobile Commerce</th>
<th>Weather</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android</td>
<td>64</td>
<td>12</td>
<td>10</td>
<td>11</td>
<td>45</td>
<td>20</td>
<td>25</td>
<td>8</td>
<td>28</td>
<td>31</td>
<td>59</td>
</tr>
<tr>
<td>iPhone</td>
<td>48</td>
<td>9</td>
<td>4</td>
<td>9</td>
<td>35</td>
<td>21</td>
<td>33</td>
<td>8</td>
<td>28</td>
<td>25</td>
<td>45</td>
</tr>
<tr>
<td>Windows</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>BlackBerry</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Total</td>
<td>116</td>
<td>21</td>
<td>14</td>
<td>20</td>
<td>83</td>
<td>42</td>
<td>60</td>
<td>16</td>
<td>59</td>
<td>57</td>
<td>108</td>
</tr>
<tr>
<td>% Total</td>
<td>97%</td>
<td>18%</td>
<td>12%</td>
<td>17%</td>
<td>69%</td>
<td>35%</td>
<td>50%</td>
<td>13%</td>
<td>49%</td>
<td>48%</td>
<td>90%</td>
</tr>
</tbody>
</table>

From this table, it is apparent that surveyed users are most inclined to use navigation, social networking and weather applications. In part, this may be due to the likelihood of having applications pre-installed on purchased smartphones. Navigation and weather apps are particularly likely to come built-in to current smartphones, perhaps accounting for the large number of affirmative responses to these categories. No distinction, however, was made between apps that had been selectively installed by the respondent and those that were included with the phone at the time of purchase.

**Attitudes towards privacy and trust**

All respondents were asked to respond to the question, “In general, how concerned are you about privacy?” The following responses were obtained:

- Not concerned at all: 5 (4%)
- Not very concerned: 23 (19%)
- Somewhat concerned: 50 (42%)
- Very concerned: 30 (25%)
- Extremely concerned: 12 (10%)
Such a distribution is roughly in keeping with previous research (13, 14) indicating that the majority of persons generally fall into a category of privacy concern generally referred to as “privacy pragmatists,” indicating that they are generally concerned about privacy, but are willing to trade privacy and personal information in return for benefits if these are perceived as reasonable. The general question about privacy concerns, in turn, was supplemented by questions pertaining to trust in the context of the specific location-aware smartphone app types that were surveyed.

Respondents were asked to respond to the following question about each surveyed app type, “Do you have any trust concerns about how the app developers/administrators or their marketers will use the information that you share with the apps you use?” Responses were categorized as follows:

- No
- Yes, a little bit
- Yes, a fair amount
- Yes, a lot
- Do not use

Figure 2 shows reported degree of trust concerns with the application types surveyed here:

It should be noted that, though respondents were asked to report their concerns only for those types of applications that they have reported using, the number of persons who reported trust concerns for each type of application was higher than that reported in Table 2 above. It is likely that persons at times also reported their trust concerns for those applications that they do not use. Here, it is evident that the greatest concerns come from social networking and mobile commerce sites. Means testing showed that survey participants had statistically significantly ($p = .05$) higher privacy concerns for these types of applications, while reporting statistically lower concerns for use of data by health and fitness and weather applications.
Actions reflecting privacy/trust awareness and concern
In addition to evaluating survey participant’s attitudes towards trust of the location-aware applications that they use, we also wanted to determine if they participate in behavior (or believe themselves to have participated in behavior) that indicates a level of general concern for privacy and use of personal data. Because it is difficult to assess how participants have acted with regard to their personal information, we use questions regarding two types of behavior in order to gain a better understanding of potential actions taken that may reflect privacy and/or trust attitudes. The first action tested is that of reading privacy policies of installed and/or used applications. Such a question is an inexact measure of privacy concern, as participants may not recall if they read an initial privacy policy prior to commencing use of an app; additionally, as noted by (Thurm and Kane, 2010), many apps do not provide privacy policies for consumers to review. However, as noted by (14) privacy policies constitute the most consistent and common method by which consumers are notified of privacy practices by app providers, thus they are used as an indicator of privacy concern by participants.

For each location-aware app type used, respondents were asked if they had read the privacy policy prior to installation and use. Response options were:

- No
- Yes
- Did not have a policy
- Don’t remember
- Do not use

Responses, again shown as percentage of persons who responded other than “Do not use” are shown in Figure 3.

FIGURE 3 Participant responses to question on whether they read the privacy policy prior to installation and use of app

Here, it is notable that the vast majority of persons who responded to this question for each app type indicated that they did not read the applicable privacy policy. Here, again, it is evident that persons tended to be more cautious with regard to social networking apps, with roughly 22% of
respondents indicating that they had read the privacy policy. Also of note, however, are the number of persons who indicate either that the app type did not have a privacy policy, or that the respondent does not remember if the app had a privacy policy. While the combined values for each fall into a range of 6-16%, perhaps most striking are the findings with respect to Mobile Commerce apps. As noted above, survey respondents indicated less trust respective to these types of applications; however, here we note that 3% of respondents indicate a lack of privacy policy from these types of application, while 13% indicate that they do not remember if these apps had a privacy policy. Here, it is evident that consumers do not always relate the presence and/or content of a privacy policy with their trust in a service, indicating that privacy policies are not adequate methods by which application providers may engender trust in their services.

Next, participants were asked to report on proactive measures they have taken regarding their trust concerns. The question was asked as follows:

- If you answered that you have some trust issues with one or more of the location-enabled apps that you use, does this impact any of your actions regarding these apps?
  - My concerns do not impact how I use these apps
  - I use a fake name for these apps
  - I do not use these apps to post pictures of myself, my friends or family
  - I do not use these apps to tag pictures of myself, my friends or family
  - I do not provide my home location information
  - I do not provide my current location information (i.e. where I am now)
  - I limit my sharing only to those in my social network
  - I do not provide my financial information to purchase goods or services through these apps
  - I use a separate email account set up specifically for these apps
  - I use these apps to receive information, but do not provide any information (such as reviews or recommendations)

Here, we are interested in determining if the self-reported concerns that users have about the apps that they use impacts the quality and/or type of data likely to be collected from their use. This is of particular interest in the area of transport as (as reported above) many agencies and organizations are exploring the use of either specifically-designed applications, or of partnerships with other collecting organizations, to supplement or enhance their ongoing data collection procedures. By examining some of the actions that people take with respect to these applications, it is hoped that we can identify if any concerns or awareness should be raised relative to potential issues with data quality based on participant use.

Results of this question are shown in Figure 4 below. It should be noted that of the 44 persons who reported that their trust concerns have no impact on how they use specified applications, seven also reported taking additional actions to limit data sharing. It is presumed that this indicates that participants have taken different approaches to different application types.
Thirty-seven persons (or roughly 31% of respondents) indicated both that their trust concerns had no impact on their use of location-aware apps, and also indicated no other actions. Responses indicated that survey participants were more likely to limit the amount of information and with whom they shared this information rather than providing fake or limited background information. This may indicate that persons using location information collected or approximated from location-sensing applications may generally be able to trust the provided information, but should be cautious about assuming that collected information is complete. A simple regression model was then run to determine if relationships could be seen between actions taken to protect information, and self-reported degree of privacy concern and use of location-sensing applications. While the model did not result in a particularly high adjusted R-squared (.329), it should be noted that both privacy concern and use of applications were seen to have a positive impact on likelihood to take specific actions regarding data privacy (at $p = .000$ and .070, respectively). Such a finding indicates the need for further analysis of influence of privacy attitude towards quality and quantity of data collected through smartphone applications, and the potential impact on transport models.

As a follow-up, survey participants were also asked if they have made any of the following privacy changes to any of the location-sensing applications that they use:

- I have turned off GPS access for some or all apps
- I have specified with whom my location and data can be shared for some or all apps
- I have turned off geotagging (i.e. automatic detection of location, which is added to the photo) on my phone's camera
- I have limited those apps that have access to my contacts, calendar or reminders
- I have limited those apps that have access to photos I have stored on my phone
- I do not share my mobile phone number with these apps

In contrast to the above, these questions are intended to determine if the user has changed or amended any settings within the app itself. Results are shown in Figure 5 below.
Here, it should be noted that settings for location-specific data services (i.e. GPS and geotagging) have the lowest likelihood of being adjusted, likely in relation to the need for these to be available to obtain the full benefits of these services. However, as above, sharing of these data with others (particularly those not in the respondent’s social network) is likely to be limited.

Finally, participants were asked about their degree of trust (on a 4-point range from “Do not trust” to “Trust completely”) of app developers and administrators with respect to the following:

• Not to sell my data to outside companies without my explicit consent
• Not to provide my data to government or law enforcement officials
• Not to track my specific location without my explicit consent
• Not to access my contact list without my explicit consent
• Not to store my data for an unreasonably long amount of time
• Not to maintain, sell or share inaccurate information

Results of this question are shown in Figure 6.
It is evident here that survey participants generally display little to no trust of app developers and administrators regarding the access and/or use of their data. Of note, as well, is that most participants indicated a similar or exact amount of trust regarding each indicator studied. These findings indicate a general level of distrust that remains relatively stable across all identified components. Of note is that there is generally less trust shown towards the actions of selling data, tracking the respondent, or providing information to government or law enforcement agencies. Respondents indicated a slightly higher degree of trust that a developers and/or administrations will refrain from accessing contacts or other data stored within the phone.

Discussion

Given both the rapid dissemination and adoption of smartphones and the wide array of location-sensing applications available, it is reasonable to anticipate that these tools have the potential for wide ranging benefits in the transportation sector. As shown above, however, some care and consideration needs to be taken as to how we treat data collected through these means. While the findings above indicate that current practices regarding the use of location-sensing (and, thus, location collection) applications allow for relatively consistent and comprehensive data to be collected, user trust concerns may begin to play more of a role in how users respond to data collection applications. The recent revelations regarding the National Security Administration’s PRISM program (in which it was revealed that the U.S. government (along with others) had gained access to internet company servers to extract communications logs) has the potential to both heighten awareness of data and location surveillance as well as erode trust in the companies that collect that data. According to The Washington Post, “The NSA prides itself on stealing secrets and breaking codes, and it is accustomed to corporate partnerships that help it divert data traffic or sidestep barriers. But there has never been a Google or Facebook before, and it is unlikely that there are richer troves of valuable intelligence than the ones in Silicon Valley (15).” Such a contention is no less true about location-specific information, and data that is invaluable for transport planning, modeling, and programming purposes is no less valuable for purposes of tracking and marketing. The indications of lack of trust in data collection, storage and use practices is revealing, as this may indicate that further actions will be taken regarding the protection of personal data as users become more confident in their ability to change settings and selectively set with whom data are shared. While this is beneficial from the point of view of privacy, it indicates the potential for smartphone-gathered location data to be evaluated carefully for indications of bias before it is used in modeling or planning applications. Correlations with the privacy-seeking behavior of users and their self-stated privacy preferences indicate that there is a class of travelers on whom it will remain more difficult to obtain comprehensive sets of travel behavior data, as such users may be disinclined to allow their data to be shared without reservations or amendment.

CONCLUSION

As shown above, the potential for collection and use of vast quantities of detailed location data from smartphones is great. The widespread adoption and use of this technology has the potential to allow for more accurate and efficient transportation planning and programming activities to occur. However, the successful use of such data is contingent upon the recognition that user attitudes and behaviors towards the collection, dissemination and use of such data must be taken into account as we strive to develop methodologies that reflect and address the concerns (particularly those regarding trust and privacy) identified. By developing transparent and open models of data access,
sharing, storage and use, some of these issues may be overcome, allowing for more value to be
added to transportation processes. It is hoped that we have here identified a number of questions
for further analysis and study, particularly regarding data quality and applications as they apply to
data collection from personal mobile devices.
REFERENCES


