Using Smartwatches for Privacy Awareness in Pervasive Environments

Peter Shaw, Mateusz Mikusz, Nigel Davies
School of Computing & Communications
Lancaster University, Lancaster, UK
p.shaw|m.mikusz|n.davies@lancaster.ac.uk

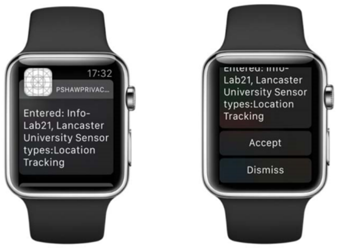
Sarah Clinch
School of Computer Science
University of Manchester, Manchester, UK
sarah.clinch@manchester.ac.uk

Future pervasive computing environments are likely to include large numbers of sensors such as cameras and microphones that are embedded in the physical environment and that can capture personal data. Such data can be used for a wide range of applications ranging from augmented cognition through entertainment to personalised advertising. However, our ability to capture personal user data far exceeds our understanding of how to manage issues of trust, privacy and consent with potentially far-reaching consequences for both individuals and society. In the PACTMAN project we are aiming to develop systems that empower users to decide when and how they should disclose personal data. Our first exploration of this space has included the development of a prototype smartwatch application that can inform users when they are entering an environment that may compromise their privacy.

Our work was informed by a small-scale on-line survey (34 respondents recruited via personal contacts and social media) and a single focus group (4 participants). We explored the extent to which participants were concerned about data capture in their environment. Though a small sample set, our results indicated that users had quite different attitudes to environmental sensing and data collection depending on the intended purpose. Security was deemed the most acceptable reason for data collection while applications that appeared to only benefit the collector (e.g. advertisments) were widely disliked. On the subject of being notified of data collection activities opinions were divided between those that wished to be made explicitly aware of such collection and those that simply did not wish to know. Interestingly, our participants were strongly opposed to any form of covert data collection and there was strong consensus that irrespective of whether explicit notifications were provided or not it must be possible for users to determine the nature of data collection taking place in any given space. These findings lay credence to the idea that attitudes to data collection are variable and that explicit notification or querying of data collection policies are important in pervasive environments.

To explore whether modern smartwatches could be used to deliver notifications of potential privacy issues we developed a prototype mobile application that used predefined maps to notify users when they were entering environments that captured personal data.

Our assumption was that maps of pervasive data capture zones could be created in a similar way to the maps used in personalisation systems such as Tacita [1]. While such an approach requires manual effort and does not protect users against deliberate covert surveillance (which would be extremely challenging) it does provide a mechanism for owners of physical spaces to inform occupants of the data they are capturing. In our prototype the map data was downloaded to the smartphone, with each region representing an area of surveillance and having an associated list of devices (e.g. Camera, Microphone) being used within the area. When a user is about to enter a region the application posts a notification listing the devices in use and providing the user with the option to accept (which suppresses future notifications for the same region) or decline (providing an opportunity for future work on surveillance consent). Additional example data about the regions could also be made available including: the size of region (map display), the legal agreement surrounding the surveillance, date agreement is valid from/to, the devices in use, and the company or owner of the data collected. The original implementation made use of the background region monitoring included in the CoreLocation framework by Apple for iOS, but after testing it was found the accuracy of background region monitoring was limited to circular regions of at least 100m, making it too inaccurate for most building/area sizes. For our prototype we subsequently used the background monitoring to trigger the active location tracking within smaller regions or Bluetooth low energy beacons to detect proximity.



Entered: Info-Lab21, Lancaster University Sensor types:Location Tracking

Figure 1: A Prototype Privacy Notification System

Our prototype draws inspiration from early ubicomp work such as [2] and shows how contemporary hardware might be used to provide users with important notifications of privacy violations. In future work we will seek to trial our smartwatch application to determine user responses to this type of privacy notification.

ACKNOWLEDGEMENTS

This work has been part funded by the UK EPSRC as part of the PACTMAN: Trust, Privacy and Consent in Future Pervasive Environments project grant no: EP/N028228/1 and through the Future and Emerging Technologies (FET) programme within the 7th Framework Programme for Research of the European Commission, under FET grant number: 612933 (RECALL).

REFERENCES

[1] Nigel Davies, Marc Langheinrich, Sarah Clinch, Ivan Elhart, Adrian Friday, Thomas Kubitza, and Bholanathsingh Surajbali. 2014. Personalisation and Privacy in Future Pervasive Display Networks. (2014), 2357–2366. DOI: http://dx.doi.org/10.1145/2556288.2557287

[2] Marc Langheinrich. 2002. A privacy awareness system for ubiquitous computing environments. (2002), 237–245.