The Internet of Things Privacy Infrastructure: Applicability, Usability, and Market Entry Strategy

James Arps, Ziheng Ni, Yiding Ou, Jingyi Zhu
Advisors: Norman Sadeh, Yuanyuan Feng, Justin Donnell, Gabriela Zanfir-Fortuna

November 21, 2019

Executive Summary

Internet of Things (IoT) technologies are devices that can collect and transfer data over the network without human-to-computer or human-to-human interaction [1]. IoT devices have become much more common in today's world. From smart doorbells to voice-controlled virtual assistants, people are using these devices to free their hands, entertain themselves and make the most of their time. Besides personal use, companies also use IoT devices such as surveillance cameras for security purposes or to conduct analytics to boost their sales. However, for customers who wander into range a wayward camera or WiFi beacon, they often have no idea what data is being collected about them, how it is processed, with whom it is being shared, or how long it will be stored.

With the General Data Protection Regulation (GDPR) having gone into effect in May of 2018 and California Consumer Protection Act (CCPA) going into effect in January 2020, companies which sell as well as use IoT devices are paying more and more attention towards protecting customers' privacy. These new laws and regulations impose new requirements on entities collecting and processing user data. Most companies are struggling to interpret them and be compliant – in one study, 54% of participants felt that implementing GDPR took longer than expected, with 80% feeling that it was equally or more difficult to comply with GDPR than with other data privacy and security initiatives [48].

The IoT Privacy Infrastructure (IoTPI), designed by researchers at Carnegie Mellon University, empowers consumers to control their privacy and supports companies' efforts to meet legal requirements or to respond to increasing privacy concerns by their users. The IoTPI contains a web interface, the IoT Portal, and an IoT Assistant (IoTA) mobile application. IoT device owners can use the IoT Portal to register their IoT resources with a geographical layer called an IoT Resource Registry (IRR), while consumers can use the IoT Assistant App to browse the IoT resources around them and perform privacy actions such as data subject access requests (DSARs).

As part of identifying potential market-entry strategies for this technology, we surveyed the legal and regulatory landscape as well as the adoption rates of different types of IoT technologies. We then conducted a pilot of IoTA marketing materials by placing two IoTA posters in Carnegie Mellon's Newell Simon Hall and measuring their engagement with passersby. The results of that exercise were mixed, with just two people out of a total of 777 scanning the QR code on the poster. By talking with those who passed by the poster but didn't scan it, we conclude that the poster was not large enough and did not draw enough attention to the QR code. Additionally, additional avenues other than posters should be pursued, as it does not appear that much of the public frequently scans QR codes on posters.

After comparing and contrasting the deployment readiness and feasibility of various products with which the IoTPI can potentially be used, we chose four use cases that we felt were the most representative and the most promising: video analytics, indoor location tracking, camera-equipped advertisements, and smart speakers. We then created IRRs for each selected use case and provided suggestions to improve the interface and smoother and expedite the process. In order to illustrate the experiences of different groups using the IoTA app, we also crafted user journeys, which informed the design of a focus group study that we performed in order to evaluate user attitudes and preferences when using the IoTA in a variety of different scenarios.

The table below briefly summarizes the recommendations made in this paper.

Category	**Recommendations**
IoTA Poster Suggestions	• Increase the size of the posters that are being hung • Place the QR code on the poster in a more prominent position to promote more frequent scanning • Add elements that break from the cool color palette used in much of the posters to draw attention to specific elements – one way this could be done is through colorful post-it notes or other elements that indicate prior human interaction with the poster and differentiate it from standard marketing materials • Write the actual phrase "Internet of Things" somewhere on the poster in order to reduce confusion about what the acronym "IoT" means • Add language or otherwise make attempts to indicate that the IoTA posters are materials for a third-party company *not* directly affiliated with the person who is doing the tracking which is advertised on the poster – our focus group participants suggested that they would not believe that the device owners have their best interests at heart
IoTA Design Suggestions	• Allow users to set a smaller discovery radius than what is currently allowed on the application, such as ten meters • Allow users to change the metric used to display the discovery radius from meters to feet • Allow users to rank the "Data Collection" categories in order of importance to them and display the results on the "In Range" page according to those preferences as well • Remove or push to the bottom categories on the "Data Collection" page for which zero IoT resources are in range • Users were confused about the colors of the IoT resources on the "In Range" page – either add a legend or have the colors be purely randomly generated • Make each IoT resource on the "In Range" page take up the full width of the screen – users were confused about why they were different sizes, and the smallest of the currently randomly-generated sizes cuts off the names of some resources • Add text at the bottom of the "In Range" screen indicating that no more resources have been found – some participants were confused by the large amount of white space when they were in an area with few or no IoT resources
IoTA Feature Suggestions	• Add a web interface for the IoTA which would be accessible by users without requiring them to download the app • Implement push notifications to make it more likely that a user opens the IoTA when they enter a space containing IoT resources; allow those push notifications to be customizable by things such as time, resource type, and data collection • Add a popover to individual IoT resources on the "In Range" page – when a resource is pressed and held, pop up a short digest of the resource along with a legend explaining what types of data is being collected by that resource • Add a "Help" page or legend to the application to explain to users what different types of tracking (such as "Presence Data") mean and provide examples

	• Add a "Recent Devices" tab which stores IoT resources that users come into contact with so that they can perform privacy actions with that resource without needing to physically travel back to its location • Develop an IoTA "widget" which could be quickly accessed by users without needing to fully open up the application and could display information such as the number of devices currently in range of the user • Add an "Explore" feature where IoTA users could explore IoT devices in their area (or around the world) via a map in order to learn more about them and even pre-emptively opt-in or -out of data collection
Outreach/Promotion	<u>Partnerships with Companies:</u> • OneTrust, due to its integrations marketplace which could serve as an example or resource for collaboration with Internet companies for the purpose of GDPR compliance • Quantcast, due to its widespread use as a consent management platform on popular websites <u>Partnerships with Governments:</u> • Belgium, due to their law mandating that surveillance cameras be tracked using an online portal • France, due to a 2017 court ruling against the advertising company JCDeceaux that said salted and hashed MAC addresses do not provide a suitable level of anonymity • Sweden, due to a prior ruling in which the Swedish DPA fined a school for improperly obtaining consent to use facial recognition cameras
Future Work	• Promote opt-in strategies as the most promising type of usage scenario for IoTA adoption • Develop a one- to two-page marketing brochure which could be given to potential partners and outlines the compliance and privacy benefits provided to companies and consumers by the IoTPI • Perform further research into the viability of creating a shareable digest which could be printed out or posted on social media by the creator of an IoT resource – the digest would contain a summary of the resource's data collection practices and privacy options • Explore different types of ratings systems which could be used to rank IoT resources in the IoTA – would users want to rate devices based on the ease of the opt-in or opt-out process, based on the perceived level of security of the device, based on expert opinions, or a combination of all of the above?