
Degrees of Agency in Owners & Users of Home IoT Devices

Marta E. Cecchinato

UCL Interaction Centre
University College London
London, UK
m.cecchinato@cs.ucl.ac.uk

Daniel Harrison

UCL Interaction Centre
University College London
London, UK
daniel.harrison@ucl.ac.uk

Abstract

Internet of Things (IoT) devices are slowly populating our homes. In this age of sharing economy and increased mobility, however, the home environment is no longer a fixed location always shared by the same people. To better understand the issues and challenges around agency and IoT use in the home, we take a pragmatic and situated approach. In this paper, we draw on our own experiences as users and identify the tensions between *ownership* and *usage*, and the economic implications there might be when sharing IoT systems with trusted people vs. strangers. We suggest the distinction between owners and users should be

Copyright is held by the author/owner(s).

Making Home: Asserting Agency in the Age of IoT Workshop

CHI 2017, May 6–11, 2017, Denver, CO.
ACM 978-1-4503-4655-9/17/05

more carefully considered in the design and research of future devices.

Author Keywords

Internet of things; IoT, agency; privacy; ubiquitous computing.

ACM Classification Keywords

H.5.m. Information interfaces and presentation (e.g., HCI): Miscellaneous.

Introduction

Our relationship with the home is changing and one driving factor lies in new ways of working. With ubiquitous computing allowing us to work anywhere and anytime, mobility and flexibility are key in many jobs [2,3]. This is enabled also by the multiple devices we own and everyday objects gaining Internet access as the Internet of Things (IoT).

Ambient Intelligence is one definition of ubiquitous computing, where computers are expected to automatically predict users' behaviours and needs and respond accordingly [5]. In their polemic paper on the evolution of ubiquitous computing, Aylett and Quigley [1] call for challenging the need for ubiquitous systems to automatically predict users' needs and inherently retain agency. The sense of agency – or feeling in control – “is a vital consideration for assessing how people experience interactions with technology” ([6],



Fig. 1. Amazon Dash button

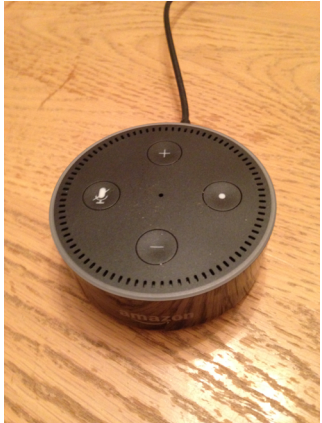


Fig. 2. Amazon Echo Dot

Together the two authors own: a Dash button (Fig. 1), an Echo Dot (Fig.2) that uses Alexa as conversational agent, an air quality and smart scale, and a Fire TV stick – a range of devices somewhat governed by living in shared, rented, accommodation.

p.1). However, the relationship between agency and IoT has not been widely studied so far, despite offering some interesting insights into our interactions with technology, which we discuss here.

Bodystorming Agency in the Age of IoT

Academics and students can be digital nomads, given their ability to work from multiple locations, as well as frequently moving between homes (or even countries). While perhaps they are a less extreme example of precariat, we believe that looking at what we know is a good starting point to uncover aspects of agency in IoT.

Thus, we – two PhD students at the time of writing – conceptualized and wrote this paper during a writing retreat in a remote location. While this context may seem irrelevant, we used this opportunity to bodystorm [7] and better understand the complexities around agency and IoT for the home using our past and present experiences in the situated context of an unfamiliar house. We are both digital nomads – often working from our shared home, but also travelling to conferences, events, and visiting our families across the world. During these trips, and at home, we have experienced several IoT devices, owned by ourselves and others, in different ways. In this paper we present our memories as diary entries and quotes from real-life conversations to discuss the tensions around agency in users and owners.

Users, Owners and Economy

Many IoT devices for the home offer a unique proposition in that they are linked to digital wallets for online purchases. While others are not directly linked to digital wallets, they can still have financial consequences. For example, by optimally regulating the

temperature in a home, smart thermostats such as Nest¹ can help lower utility bills. However, as optimal as that might sound, the reality of interactions with these IoT devices and the financial and economic implications are far more nuanced.

OWNERSHIP & USE OF IOT DEVICES IN A FAMILY

Dec. 2016. Cambridge, UK. Danny, "Marta, I've set up the Dash button for Listerine in our en-suite. Don't press it!". About 30min later, Danny says: "What?! I just saw an order confirmation for mouthwash. Did you press it?!" Marta: "Hell no, I'm scared of that thing!" A few hours later, Danny: "Great. I forgot to cancel the order and now it's been dispatched!". [Fig. 1]

Jan. 2017. Cambridge, UK. Marta: "Danny, did you ask Alexa to buy you a PlayStation using my account?! I found a PlayStation in my Amazon basket – lucky for me I noticed before I went to check-out!" [Fig. 2]

Possessions are often shared within families, but this does not usually extend to things such as wallets and user accounts. The examples above arose because of a mismatch between the *user* and the *owner* of the device within a family: in the first example, Danny suspected Marta had pressed his Dash button² to play a trick; in the second one, Danny retaliated by asking Alexa to put a PlayStation into Marta's Amazon basket via her Echo Dot³. Both devices were in shared spaces in the home, and the Echo was even used as a shared

¹ <https://nest.com/>

² <https://www.amazon.co.uk/b?ie=UTF8&node=10833773031>

³ <https://www.amazon.co.uk/Amazon-Echo-Dot-Generation-Black/dp/B01DFKBL68>

device, despite being owned by, and linked to, Marta's Amazon account.

Unsurprisingly, given Amazon's business, these devices offer seamless purchasing of goods, but neither require much in the way of authentication from the user. This means others may take advantage and accidental purchases can easily be made. A similar scenario could have taken place for example in a family home with teenagers, or in a shared student accommodation. An obvious, but perhaps costly, solution could be to include authentication (e.g. fingerprint or voice recognition) or design frictions [4], which could also be used to recognize users on shared devices where the owner and the user are different people.

OWNERSHIP & USE OF IOT DEVICES IN A SHARING ECONOMY

Sept. 2014. Seattle, WA. Danny arrives in an Airbnb for a week-long stay. Host: "...and this is the smart TV. We've got cable, and one of the previous guests left his Netflix account signed in, so feel free to use it!".

Oct.-Dec. 2014. Atlanta, GA. One day on Skype, Marta: "Hey Dan, how are you?" Danny: "All good, but I'm getting frustrated with my Nest – for some reason it keeps turning the air conditioning on and it's not hot outside! Not sure if it's my Airbnb host changing the temperature via his app. Even if I can change the settings, I have no control over it!"

These two examples are again related to a mismatch between *owner* and *user*. In the first example the SmartTV hardware was clearly owned and maintained by the Airbnb host, who was perhaps taking advantage of one of his prior guests. In the second example, most would consider Danny to be the user of the Nest – he

was staying in the property alone and would have total control with a traditional thermostat. Normal use of the Nest removes some agency from the user, as it controls the heating in attempts to conserve energy. An additional challenge arose, as Danny was unable to use the smartphone app to control the Nest and suspected his host was remotely controlling the device to save energy. More likely, the Nest could have been confused as a result of trying to learn a consistent pattern from previous guests, who may not have had consistent preferences amongst each other. This disconnect between owner and user can cause tensions in the shared economy, perhaps even resulting in legal consequences in the Netflix example.

OWNERSHIP & USE OF DIGITAL CONTENT THROUGH IOT DEVICES

July 2016. Cambridge & Hampshire (UK). Danny texting his nan, Glad: "Are you reading 'The End of the World Running Club on your Kindle?'". Glad: "Yes... why?". Danny: "I bought it for myself last week and I saw that someone had started reading it!". Glad: "Oh, I checked that it was at 0% and I thought I could read it".

Jan. 2017. London & Cambridge (UK). Marta starts playing music on her phone as she walks to the station, then receives a text from Danny, who is at home (listening to music, through the Echo Dot): "Amazon music is streaming on another device, would you like to stream here instead? I said no... enjoy your music!!"
[Fig. 3]

The examples above illustrate tensions when multiple users attempt to access the same digital content. In both cases the digital libraries (eBooks and music) are deliberately shared between multiple users, but can

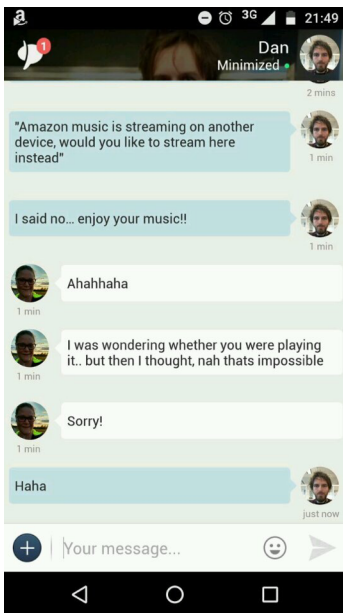


Fig. 3. Conversation between Danny and Marta regarding their use of Amazon music.

only be used by one user at a time, causing conflict between multiple users trying to access the same resource. In each case, there is a *primary user* – generally the *account owner*, along with a *secondary user* – a guest. While some solutions exist, with shared family accounts, this might not be applicable to context where the various users are unknown to each other. Take the case of hotels and guest houses that have lending libraries and book collections available to guests – if not all users are equal, how would access and thus agency be negotiated in this case? Thinking beyond these examples, the *owner* and the *primary user* may not always be the same person. For example, how should agency be distributed when an IoT device such as Amazon Echo, is used as an accessibility tool by a person with a disability, but the account owner is a family member?

Discussion and Conclusion

Drawing from our own experiences, in this paper we have provided real-life examples of the tension around agency between *owning* and *using* IoT devices.

While mobile computing was never intended to be shared [1], IoT devices for the home, become part of the furniture, and as such can be inherently sharable. The sharing aspect of IoT devices is a common thread in our examples here, and highlights critical differences when sharing agency with people you trust vs. strangers. This in turn can have positive or negative financial consequences if not appropriately moderated by the owner. Currently, at least some IoT devices are designed to allow some degree of shared agency among users, however certain functions (e.g. cancelling an order) are only granted to the owners. Usage over time is another critical aspect for determining agency in

IoT devices. The example we provided about the Nest demonstrates how in a fast-paced sharing economy of individuals interacting with IoT, giving agency to a device can be counter-productive. The cases we presented in this paper are not intended to be exhaustive, but illustrate the case to better consider human agency around use and ownership for shared IoT devices, especially over time.

Provocation

Through multiple examples, we have demonstrated how IoT devices in the home can emphasise differences amongst users and have negative consequences due to their shared nature. Borrowing one of George Orwell's famous statements, we would like to conclude with a provocation that sums up our argument: *all users are equal, but some are more equal than others.*

During the workshop, we would like to encourage the discussion around this statement, and the implications it has around feelings of trust. How should these devices be designed to take into account multiple users that have different degrees of agency?

Biographies

Marta E. Cecchinato is a PhD student at UCL researching the use of technology in both the home and work environments for boundary management. She is interested in strategies users rely on to ensure a sense of control and agency.

Daniel Harrison is a PhD student at UCL and researcher at Microsoft Research (Cambridge, UK). He is interested in people's everyday lifestyle and how people collect digital and physical objects in the home.

References

1. Matthew P Aylett and Aaron Quigley. 2015. The Broken Dream of Pervasive Sentient Ambient Calm Invisible Ubiquitous Computing. *CHI Extended Abstracts on Human Factors in Computing Systems*, 425–435.
2. Marta Cecchinato, Anna Cox, and Jon Bird. 2016. Work-Life Balance through Tangibles and the Internet of Things. *CHI2016 Workshop on Tangibles 4 Health*.
3. Marta E Cecchinato, Anna L Cox, and Jon Bird. 2015. Working 9-5? Professional Differences in Email and Boundary Management Practices. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 3989–3998.
4. Anna L Cox, Sandy Gould, Marta E. Cecchinato, Ioanna Iacovides, and Ian Renfree. 2016. Design Frictions for Mindful Interactions: The Case for Microboundaries. *CHI Extended Abstracts on Human Factors in Computing Systems*, 1389–1397. <http://doi.org/10.1145/2851581.2892410>
5. K. Ducatel, M. Bogdanowicz, F. Scapolo, J. Leijten, and J. Burgelman. 2010. Scenarios for Ambient Intelligence. *Office for official publications of the European Communities*.
6. Hannah Limerick, David Coyle, and James W Moore. 2014. The experience of agency in human-computer interactions: a review. 8, August: 1–10. <http://doi.org/10.3389/fnhum.2014.00643>
7. Antti Oulasvirta, E Kurvinen, and T Kankainen. 2003. Understanding contexts by being there: case studies in bodystorming. *Personal and Ubiquitous Computing* 7, 2: 125–134. <http://doi.org/10.1007/s00779-003-0238-7>