Human Data Interaction in IoT: The Ownership Aspect

Afra Mashhadi
Bell Laboratories
Alcatel-Lucent
Dublin, Ireland
afra.mashhadi@alcatel-lucent.com

Fahim Kawsar and Utku Günay Acer
Bell Laboratories
Alcatel-Lucent
Antwerp, Belgium
{fahim.kawsar, utku_gunay.acer}@alcatel-lucent.com

***Abstract*—As Internet of Things (IoT) becomes a growing reality, more ubiquitous devices are embedded in our daily lives, serving us in a broad range of purposes in everyday life from: personal healthcare to home automation to tailored smart city services. These devices primarily collect data that is about or produced by people, be it street noise level of a neighbourhood, or the energy footprint of an individual's home or her location and other situational context. As this unprecedented amount of data is collected, we are challenged with one fundamental research question: *who owns this data and who should have access to it?* Specifically, the emergent of the Human Data Interaction (HDI) topic which aims to put the human at the centre of the *data driven industry*, calls attention to the IoT community to address the data ownership aspect more carefully. In this note, we offer a reflection on the challenges that IoT faces in regards to the data ownership in HDI and advocate the roles that both ordinary people and industries must play to best answer those challenges in shaping the IoT landscape.**

I. Introduction

We are observing a significant metamorphosis of our computation driven experience uncovered by a plethora of open source hardware i.e. sensors and actuators resulting in more and more connected objects embodied with intelligence. As such, our physical space now represents an ecological synergy of connected objects augmented with awareness technologies. This unfolds a range of imaginative possibilities to discover, manage, compose, coordinate, and control physical space to realise personalised and coordinated behaviour within and across devices and provide the foundation for the Internet of Things (IoT). For instance, we now interact with our clothes to exchange emotion, with our furniture for personalised information services, with our umbrellas for weather forecast, etc. In fact, recent years have seen a sharp rise in the number of ubiquitous devices and the market is growing increasingly as IoT applications are becoming mainstream thanks to crowd-funding platforms such as KickStarter[1] and strong initiatives from large industrial companies. These devices facilitate our lives and will be everywhere, from home automation to public spaces, and used by everyone. The common facet of all these devices is that they all collect data that is produced *by* or *about* people. This data is either explicitly produced by users themselves, for example sharing their location while running through wearable accessories, or is implicitly inferred by the sensing infrastructures in cases such as monitoring residential energy consumption or the noise level of an area. As this unprecedented amount of data is collected, we are faced with a fundamental research question regarding data ownership, in other words *who owns this data*, that is produced by this swarm of connected objects, and *who has consent to access it* ?

Recently in an effort to address this research question in a broader context of data analytics, the topic of Human Data Interaction (HDI) [1] has emerged. HDI refers to the broad topic of providing access and understanding of data that is about individuals and information on how their collected data affects them, by placing human at the centre of the *data driven* applications. Being an inter-disciplinary field, HDI brings together efforts from domains of databases, computer science, visualisation and interaction design along side law, psychology and behavioural economics in an attempt to define a human centred framework and design guidelines for future data driven applications. In the domain of IoT and more specifically in pervasive computing research, various studies have addressed the relationship between human and data through the data accessibility lens [2]–[5]. In [4], the authors review the access control and role functionalities of some off-the-shelf home devices such as a wireless scale, and a variable colour lighting system. They highlight the deficiencies of the current state of the access control policies for these devices. In particular they observed that users lack awareness on who has accessed their devices due to missing intelligible feedback. Brush et. al. [2] suggest that simple design guidelines such as proximity-based trust can solve some security challenges in the domain of home automation. In [3], [5] authors address the access control in terms of simple predefined groups (e.g., kids, parents, etc) as well as temporary access provision for guests. In [6], the authors highlights the need for a better visibility to the home network noting the privacy concerns. Finally [7] discusses an extensive view of consent in the field of ubicomp and proposes guidelines for rebalancing the focus from the system to the users.

While these solutions can provide sufficient access control for individual technologies, the problem of data ownership in the IoT arises as each crowd funded device in the market relies on its own individual black-box application to interact with the device. As such causing fragmentation in data ownership. Furthermore, as the IoT scales and smart cities become a reality, addressing data ownership and accessibility becomes ever more critical. For instance, imagine the local government has placed surveillance cameras and sensors on the street lamps

[1] http://www.kickstarter.com/

in you neighbourhood to improve public safety, and to monitor the air pollution level for offering better environmental awareness to their citizens. However, the collected data is later sold to or shared with a third party company that operates as state agents. In this example, *who owns this data? And who should be able to access it? Should people in the neighbourhood have consent to decide with whom their data can be shared with or sold to?*

In the rest of this note, we discuss the challenge of the data ownership in the IoT space taking an analytical stance and propose three models to instigate a dialogue on the roles that both individuals and industries can play in this new connected eco-system.

II. A Two-Dimensional View of the IoT Space

Keeping the human consent at the centre of data ownership in IoT is an endeavouring challenge. At its core, resides the question of how a technology whose backbone consists of objects and aims to connect devices together, can account for human interaction. Indeed the literature on consent draws from multiple disciplines such as law [8], computer science [7], sociology and design [9], and psychology [10]. The common point that all these multiple disciplines concur with, is the need to enable users to review/withdraw and interact with their data (e.g., through visualisation). However the IoT domain differs greatly from the traditional data collection methods in practice. To understand these dynamics better, we present a view of IoT space from two dimensions:

1) *Functional Scope:* Functional scope defines the operating mode of the connected objects, and ranges from self-contained to infra-structured ones.
2) *Spatial Scope:* Spatial scope defines the operating space of a smart object which can be either private or public.

A self contained connected object is independent of any local infrastructure (e.g., a gateway) and is capable of perception, reasoning and decision making autonomously and can operate in a private space (e.g., a cooking pot, a personal health care monitoring device, etc.) or in a public place (e.g., a smart elevator, a smart vending machine, etc.). An infra-structured connected object is a part of larger collection of physical objects that work collectively to attain a specific purpose in a private space (e.g., a home automation system) or in a public space (e.g., smart city services). Figure 1 illustrates this two dimensional view of the IoT.

To highlight the challenge that is facing the IoT in regard to HDI, Figure 2 illustrates the sensitivity of the collected data versus the consent given to the users to interact with their data, for the IoT space described above. As presented in this figure, there are range of connected objects which rely on collecting sensitive data about the user (e.g., connected smart home) but at their current implementation they provide the users with little consent to review and interact with this data. For example, in the domain of the connected home, if the data of users daily behaviour (such as energy usage) is shared with other companies, it can lead to invasive advertisement as well as potential risk to the household. Indeed consent is defined as "the primary means for individuals to exercise their autonomy and to protect their privacy" [11]. Therefore the more private and sensitive the collected data is, the higher the provided consent should be.

Fig. 1: A Two-Dimensional View of IoT Space

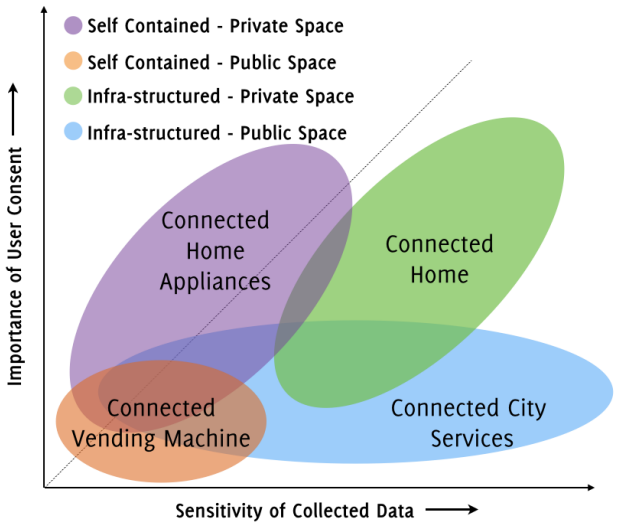

Fig. 2: The Consent View of the IoT space.

III. Ownership Models for the IoT Space

Considering the view of IoT presented in the previous section, we foresee multiple models of data ownership of varying granularity - i) Pay-Per-Use Model, ii) Data Market Model and iii) Open Data Model. In the following, we discuss these models and their implications into the IoT space.

A. Pay-Per-Use Model

As future objects such as appliances become connected and aware of their current state and usage patterns (i.e., state full objects), the collected data from these objects can be used to interpret information about the users beyond their original purpose. For example, consider a smart chair which is able to remember your desired configuration. While the data is originally collected to provide this service, should the manufacturing company be able to use this data for other purposes too (e.g., selling your weight information to a third party company). The current state of the IoT and massive number of crowd founded appliances in the market lacks users consent regarding *how* their data is used and *how much* is worth. To address this challenge, we propose a model in which human can gain monetary benefit from the data they share through their smart appliances, through a Pay-Per-Use model [12]. In this model the user would be able to rent a smart appliance and only pay for it based on their usage as the manufacturing company collects the data from the appliances. Indeed, such payment models have been already proven to be popular in the automobile industry where the users can lease their desired car, also pay for its insurance depending to their use[2]. Indeed a recent survey by Lynx Research Consulting has shown an increase in the popularity of such insurance schemes despite the privacy concerns[3]. Granting similar model for smart appliances allows the manufacturers to monitor how their products are used thus enabling them to know what are the important features to improve, keep or discard. Moreover, it enables the manufacturing companies to apply a better repair and warranty models which would take account for the usage of the appliance and its deviation from the recommended guideline. A challenge that arises in here is on the affordability of such a payment model as it requires the companies to have the necessary capital, as well as the risks of frauds through tempering with the usage data. However, given the subscription based models are becoming increasingly popular in the IoT space, (e.g., Tado Thermostat[4]), we concur that connected object manufacturer would consider this model to balance their value proposition with respect to perceived affordance of the consumers. This might also be critical to overcome the barrier of *lacking consumer awareness*, a fundamental blocking element for penetration of the IoT devices in the mass market, especially for the consumer focused ones.

B. Data Market Model

The IoT in private spaces such as residential home, semi-private office spaces goes beyond simply a collection of connected objects and opens up many privacy considerations to account for. Data streamed off devices in home regarding energy or water usage has so far been handled by companies which treat the users as clients only with no say on how their data should be used. However, we believe that given a transparent framework and regulations, many users would be willing to share their data [13]. As such, we propose the notion of Data Market as an instrument to enable users to share their personal data locally and globally with monetary benefits, i.e., an individual can trade data produced at her personal space with interested business entities. Such model is currently being considered by a number of data exchange companies, where monetary incentives are offered to end users for correcting erroneous sensor data[5]. The challenge in this case is how to design future infrastructure so to make users aware of the commodity of their data along with the risks of sharing it.

C. Open Data Model

The data ownership becomes a much bigger challenge as we step outside specific domains such as healthcare and home automations and look at the bigger picture of smart cities. To keep the IoT ecosystem alive [14], one needs to be able to reuse the already deployed devices for purposes beyond the primary intention. One fundamental challenge that arises in this case is the *role identification* that is beyond the classic access control roles. First, we need to be able to identify who are those that are affected by the collected/inferred data from the sensors (e.g., the sensors deployed in the neighbourhood). Are the roles limited to the physical proximity of the deployed devices? And finally what are the relationships amongst the roles? Furthermore, once the roles identified how can we provide simple means of *interactions with the data*, such that ordinary users can gain access to how their data is being used and control for it. We advocate Open Data Model with *intention integrity*, that is ordinary users should be capable of wilfully access their data captured by public devices, and the data must be used only to achieve the intended operation, and any inferred information for other intentions must be first approved by the users.

IV. Connecting the Device Space with Ownership Models

In the previous two sections we have described a two dimensional view of the IoT from functional and spatial perspectives, and three ownership models for the data generated by the IoT devices and services. Although we do no advocate a set of policies for connecting these two facets, in this section we offer a set of guidelines that IoT device/service providers can consider while designing their business model. Our objective here is to provide a balance between the value proposition, consumer awareness and data ownership for the future IoT services. These guidelines are visually depicted in Figure 3.

1) *Self Contained Connected Objects in the Private Space:* For this class of connected objects we argue that a Pay-Per-Use model would be appealing for the consumers as well as for the device and service providers. For example, a smart vacuum cleaner could be offered for a nominal price upfront, however the consumers are billed every month or quarter on the basis of the usage quantity and quality. As discussed in the earlier section, this model is lucrative not only for the consumers considering monetary benefits, but also for the service providers as they will have better awareness of their service and product usage, customer segmentation, and for designing future functionalities of the product that are most useful for the consumers.

[2]Pay-as-you-drive insurance schemes allow the drivers to attach a device to their car that records the use of the car and sends it to the insurance company.

[3]http://digitaljournal.com/article/357201

[4]http://www.tado.com

[5]http://developer.centralindex.com

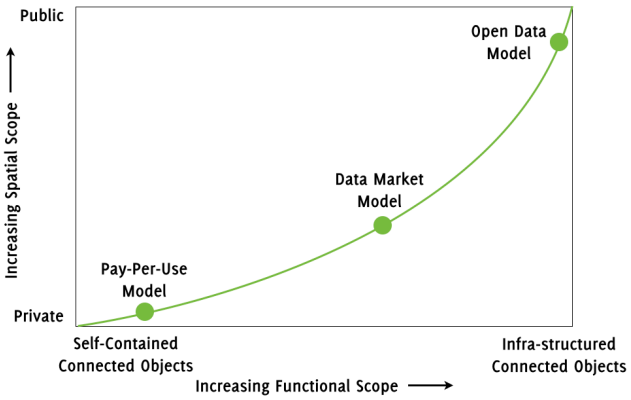

Fig. 3: Data Ownership Models for the IoT Space

2) *Self Contained Connected Objects in the Public Space:* For this class of connected objects we also argue for a Pay-Per-Use model. However, given the spatial aspect and common use of these objects, consumers can be offered a small discount as a value added service in exchange of their data. Taking a smart vending machine example, this means that the machine records an individual's purchase history to offer a recommendation with a small discount to promote a new item or less popular items. This is also a win-win situation for the both the manufacturer as well as for the consumers. In this particular example, the manufacturer can use the purchase history of the individuals with predictive analytics to plan stock refill to ensure optimise sales.
3) *Infra-structured Connected Objects in the Private Space:* For this class of objects, we promote a Data Market model, where individuals can trade their data either for monetary incentives, or other tangible or intangible services. For example, data produced by a residential energy monitoring system, can be traded with the utility company for a discount, or a free repair / inspection service etc. The service provider can use the collected data for a variety of purposes, e.g., exchanging insight from the data with the utility companies for better resource planning, and/or with home appliance manufacturers for targeted advertisement.
4) *Infra-structured Connected Objects in the Public Space:* For this class of objects, we advocate a completely open data model where monetary incentives are not mandatory but individuals should be fully aware of their data, and should be able to control who can use their data and how. As such, we foresee that the role of policy enforcement from the government is very critical.

V. Outlook

In this note, we put forward three ownership models for the emerging Human Data Interaction in the IoT space as an attempt to initiate a dialogue in the community. We would hope that this note stimulates others to consider how to empower the users to get more out of their shared data, enabling them to be an important part of the IoT ecosystem. We argue that there is a strong need for communication between the industries involved and the users regarding data ownership aspect and the research community needs to address this sensitive issue carefully to ensure that the Internet of Things does not fall short of its potentials.

References

[1] R. Mortier, H. Haddadi, T. Henderson, D. McAuley, and J. Crowcroft, "Challenges & opportunities in human-data interaction," in *University of Cambridge, Computer Laboratory*, 2013.

[2] A. B. Brush, B. Lee, R. Mahajan, S. Agarwal, S. Saroiu, and C. Dixon, "Home automation in the wild: challenges and opportunities," in *Proceedings CHI '11*, 2011, pp. 2115–2124.

[3] M. L. Mazurek, J. Arsenault, J. Bresee, N. Gupta, I. Ion, C. Johns, D. Lee, Y. Liang, J. Olsen, B. Salmon *et al.*, "Access control for home data sharing: Attitudes, needs and practices," in *Proceedings of the CHI'10*, 2010, pp. 645–654.

[4] B. Ur, J. Jung, and S. Schechter, "The current state of access control for smart devices in homes," in *Workshop on Home Usable Privacy and Security (HUPS)*, 2013.

[5] T. Denning, T. Kohno, and H. M. Levy, "Computer security and the modern home," *Commun. ACM*, vol. 56, no. 1, pp. 94–103, Jan. 2013.

[6] R. Mortier, T. Rodden, P. Tolmie, T. Lodge, R. Spencer, J. Sventek, A. Koliousis *et al.*, "Homework: Putting interaction into the infrastructure," in *Proceedings of the 25th annual ACM symposium on User interface software and technology*. ACM, 2012, pp. 197–206.

[7] E. Luger and T. Rodden, "An informed view on consent for ubicomp," in *Proceedings of the 2013 ACM international joint conference on Pervasive and ubiquitous computing*. ACM, 2013, pp. 529–538.

[8] Y. Bakos, F. Marotta-Wurgler, and D. Trossen, "Does anyone read the fine print? testing a law and economics approach to standard form contracts," in *Testing a Law and Economics Approach to Standard Form Contracts (October 6, 2009). CELS 2009 4th Annual Conference on Empirical Legal Studies Paper*, 2009, pp. 09–40.

[9] B. Friedman, P. Lin, and J. K. Miller, "Informed consent by design," *Security and Usability*, pp. 495–521, 2005.

[10] V. C. Plaut and R. P. Bartlett III, "Blind consent? a social psychological investigation of non-readership of click-through agreements." *Law and human behavior*, vol. 36, no. 4, p. 293, 2012.

[11] L. Curren and J. Kaye, "Revoking consent: A blind spotin data protection law?" *Computer Law & Security Review*, vol. 26, no. 3, pp. 273–283, 2010.

[12] D. Fitton, V. Sundramoorthy, G. Kortuem, J. Brown, C. Efstratiou, J. Finney, and N. Davies, "Exploring the design of pay-per-use objects in the construction domain," in *Proceedings of the EuroSSC'08*, 2008, pp. 192–205.

[13] D. Foster, M. Blythe, P. Cairns, and S. Lawson, "Competitive carbon counting: can social networking sites make saving energy more enjoyable?" in *Proceedings of the CHI'10*, 2010, pp. 4039–4044.

[14] S. Leminen, M. Westerlund, M. Rajahonka, and R. Siuruainen, "Towards iot ecosystems and business models," in *Internet of Things, Smart Spaces, and Next Generation Networking*. Springer, 2012, pp. 15–26.