The value of personal data in IoT

Burgess, Lucie; Skatova, Anya; Ma, Sinong; McDonald, Rebecca; Maple, Carsten

DOI:
10.1049/cp.2019.0150

Document Version
Peer reviewed version

Citation for published version (Harvard):
Burgess, L, Skatova, A, Ma, S, McDonald, R & Maple, C 2019, The value of personal data in IoT: industry perspectives on consumer conceptions of value. in *Living in the Internet of Things (IoT 2019).* Institution of Engineering and Technology, Living in the Internet of Things, London, United Kingdom, 1/05/19. https://doi.org/10.1049/cp.2019.0150

THE VALUE OF PERSONAL DATA IN IOT: INDUSTRY PERSPECTIVES ON CONSUMER CONCEPTIONS OF VALUE

Lucie C Burgess[*,1,2], *Anya Skatova*[3,4,5], *Sinong Ma*[5], *Rebecca McDonald*[4,6], *Carsten Maple*[5]

[1]Digital Catapult, London, UK
[2]Helix Data Innovation, London, UK
[3]School of Psychological Science, University of Bristol, Bristol, UK
[4]Warwick Business School, University of Warwick, Coventry, UK
[5]Warwick Manufacturing Group, University of Warwick, Coventry, UK
[6]School of Economics, University of Birmingham, Birmingham, UK
*lucie.burgess@helixdata.ai, *anya.skatova@bristol.ac.uk

Keywords: PRIVACY, CONSUMER PROTECTION, INFORMATION ASYMMETRY, BUSINESS MODELS, DATA ETHICS

Abstract

Personal data is an essential component of business models using the Internet of Things (IoT). Massive volumes of personal data are being recorded and analysed about consumers, despite them having limited understanding about how it affects them. Perceptions and preferences in this space influence how consumers choose to interact with the IoT, to a large extent. Yet little is understood about how industry perceives the views of consumers regarding the use of their personal data. To address this gap, we conducted three workshops with IoT industry stakeholders exploring their perspectives of consumer conceptions of the value of personal data in IoT. From the workshops, three overarching analytical themes emerged: (1) A perception of a significant gap between industry and consumers' understanding of what personal data is, who owns it, how it is used in IoT products and how it drives value in IoT businesses; (2) Perceived imbalances of power between industry and consumers in the control of and value extracted from personal data, with implications for inequalities between different consumer groups; and (3) A need for greater education and transparency for consumers, and for industry, about how personal data can be used. We develop a tentative five-point manifesto for the use of personal data in IoT, and conclude that a deeper understanding of consumer perspectives by industry would be positive for the ethical development of the IoT.

1 Introduction

The collection, analysis and use of identifiable data from individuals, known as personal data, underpins the business models employed by many organisations utilising the Internet of Things (IoT), and is essential to enable these businesses to trade. The growth of the IoT has been hard to predict and estimates have varied [1], therefore exact numbers should be treated with some caution. However, all commentators expect significant growth of the IoT sector, and the rapid evolution of devices and services that have already been brought to market supports such opinions. Specialist market analyst IoT Analytics reports that the number of connected devices that were in use worldwide in 2018 exceeded 17 billion [2], with the number of IoT devices at 7 billion (this definition excludes smartphones, tablets, laptops and fixed line phones). It estimates that by 2025 there will be 34.2 billion connected devices, of which 21.5 billion will be IoT devices. The uptake of IoT is seen in many different application domains including agriculture, transport and mobility, healthcare, manufacturing, logistics and consumer products. The focus of this research is the latter.

An estimated 17 billion transactions involving personal data take place on the Internet every day in the UK alone [3]. Existing businesses are transitioning from mass-market operating models to consumer-centric models, and swathes of new organisations are building their business in this way. An increasing array of IoT-connected devices – including increasingly-sophisticated smartphones, fitness trackers, home appliances, smart ticket gates at train stations and airports, car telemetry systems, 'smart' energy meters and even connected clothing – consume and produce vast quantities of personal data in the IoT to personalise retail experiences, optimise journeys, improve health, help manage finances and minimise energy consumption [4]. According to IDC's Worldwide Internet of Things Forecast 2017-2021 [5], 57% of organisations worldwide see the Internet of Things as strategic to their business; another 23% of organisations see IoT as transformational to their business.

By underpinning these business models, personal data hold considerable value for the companies that deliver IoT products and services to consumers. According to Transparency Market Research [6], in 2017 personal data accounted for 36% of direct data sales, both legal and illegal, in a global data market worth $250Bn. According to the European Commission, the EU-28 data market will be worth €79.6Bn in 2020 [7], valuing

personal data transactions at approximately €29Bn annually. The wider EU-28 data economy is expected to be worth €430Bn by 2020 [7], of which personal data contributes materially to almost every sector. Such unprecedented personal data collection and use at huge scale also causes significant privacy concerns for consumers [8-9].

Set in the context of new legal obligations brought about by the introduction of the General Data Protection Regulation (GDPR) in the EU, and the upcoming ePrivacy Regulation, businesses need to consider the opinions of their consumers, and in particular their fears around security and privacy. This is particularly important when consumer trust towards data-driven companies is lowered in the light of events such as the Facebook and Cambridge Analytica episode, discussed further below. How organisations engage and understand consumer perceptions is not clear: there is a lack of research on industry understanding of consumer perceptions, and the impact that this has on their business models.

This paper reports on the findings of three round-table sessions, held with a total of 32 IoT industry stakeholders, exploring consumer conceptions of the value of personal data and privacy and the implications for IoT companies. We describe the methodology for the round-table discussions and present themes emerging from the workshops. We focus our discussion on the overarching 'analytic' themes articulated by the IoT business community whilst briefly highlighting 'IoT data' themes which represent novel areas of the discussion relevant to IoT personal data. Our research presents a starting point for understanding how consumer conceptions of value might be embedded into IoT business models and personal data practices, allowing for companies to harness economic value from personal data in the IoT, in an ethical manner that preserves consumers' rights to privacy. We discuss such possibilities arising from our research, and we present a tentative manifesto for future action, to enable IoT businesses to create value from personal data whilst preserving privacy, enhancing transparency and enabling consumer trust. Finally, we explore potential future research directions.

2 Background and Existing Work

2.1 Novelty of the research: Much of the existing literature investigates the IoT from the perspective of enabling technology, architectures, privacy and security, applications and economics [10-12].

There have been numerous studies on consumer perceptions of IoT in relation to personal data. For example, Shin [13] explores the relationship between consumer experiences and perceptions of quality in IoT, including personalisation; Hsu and Lin [14] investigate the link between concerns for information privacy and consumer adoption; Chang et al [15] studied the influence of IoT product characteristics on consumer buying behavior and found that concerns about security and privacy was one of six key characteristics influencing purchase intentions.

Researchers have investigated the relationship between consumer privacy concerns and collection or release of personal information in the digital economy. Malhotra, Kim and Aggarwal 2004 [16] developed a causal model for privacy concerns online and demonstrated its relevance to data collection, control and awareness in the context of e-commerce. They acknowledged the potential for '*opportunistic behaviours'* from companies, such as an inequitable exchange of personal information. Researchers have studied the privacy paradox of the social web [17-18], which states that while internet users are concerned about privacy, their online information disclosure practices do not mirror those concerns; and the *'new privacy paradox'* of young people, who are more privacy-aware in their practices compared with previous generations yet their prolific use of social media means they must disclose information on social media sites *'despite the fact that these sites do not provide adequate privacy controls'* [19]. Researchers have also investigated privacy and security concerns relating to IoT devices, technologies and infrastructures [20].

Acquisti, Taylor and Wagman 2016 [8] investigated the economic value and consequences of protecting and disclosing personal information online, and on consumer understanding and decisions regarding the trade-offs associated with the privacy and the sharing of personal data online. They stated that *'extracting economic value from data and protecting privacy do not need to be antithetical goals'*. Zhou and Parimuthu 2015 [21] proposed an economic model of differential privacy in IoT based on individual context and need, with which our findings are broadly consistent. Kim et al 2019 [22] explored 'privacy calculus' in the IoT, the extent to which perceived risks from loss of personal data and perceived benefits (e.g. from personalization) to consumers interact to provide economic value to businesses, again with which our findings are broadly consistent.

Lu, Papagiannidis and Alamanos 2018 [23] reviewed the business literature on IoT from both the user and organisational perspectives, providing a novel view of both sides of the equation. From the user perspective, they identified privacy concerns as a key theme - *'On an individual level, privacy is regarded as a double-edged sword: users consider privacy controls as a protection of their personal information, but the risk of privacy invasion could be a barrier to IoT acceptance'*. From an organizational perspective, security, accountability and ethical design was viewed as a key theme.

Our research enriches the existing literature by exploring industry perspectives about how consumers perceive and value the use of their personal data in the IoT, and the potential impact of these perceptions on innovation in the IoT.

2.2 Information asymmetry in personal data: the collection and use of personal data in digital economies, and in IoT particularly, is not always transparent to consumers, who are themselves the originators of personal data [8]. This lack of transparency reflects an information asymmetry between industry and consumers and therefore *'consumers' ability to*

make informed decisions about their privacy is severely hindered' [8]. We assert that the scale and complexity of the collection and use of personal data in IoT make this information asymmetry between industry and consumers even more pronounced, with profound consequences for IoT business value and consumer protection. It is not clear whether companies take into account this potential lack of transparency and information asymmetry in the design of the IoT services they offer, or the extent to which they take the consumer perspective into account when designing personal data processes. While consumers may benefit from access to free or paid for services, the value from such downstream personal data transactions is typically not available to consumers, denoting a value asymmetry as well as, and arguably resulting from, the information asymmetry. Zuboff 2015 [24] has gone so far as to dub the mining of personal data as *'behavioural data mining'* and the market models employed by some IoT businesses as *'surveillance capitalism'*.

2.3 Aims of this study: given the potential information asymmetry between industry and consumers, we anticipated that industry stakeholders and consumers would have divergent views about the use and value of personal data in IoT. We suggest that this information asymmetry might persist despite the recent introduction of the GDPR which places a greater responsibility on companies to explain clearly and simply to consumers for what purpose their data is collected and how it is used. The aim of this study was therefore to understand industry perspectives on consumer perceptions of personal data value in the current and future IoT environment, highlight potential areas of convergence and divergence and explore their potential impact on the competitiveness of IoT businesses and consumers themselves.

2.4 Importance of the research: it is in the interests of industry to understand how their perspectives might differ from consumers given the potential for information asymmetry to disadvantage consumers. The considerable fines of up to 4% of global turnover associated with the worst offences under GDPR provide one compelling reason. Not only do consumers increasingly care about ethical and sustainable business practices and a lack of transparency about personal data practices might be a reputational risk to IoT companies; but also because *'the lack of consumer confidence in online privacy has been identified as a major problem hampering the growth of e-commerce'* [16]. With regard to the Internet of Things, a recent study [25] asked consumers around the world what they most fear about a more connected future: a significant percentage of people responded that it was a loss of privacy (45%). Such fears will necessarily restrict adoption of IoT devices, and indeed one study from consulting firm Deloitte [26] shows that 11% of people are holding back from buying connected devices because they do not want their usage data accessed by companies. In addition, taking into account consumers' perspectives on privacy might be beneficial for the business: it is worth pondering whether industry 'may be able to leverage privacy protection as a selling point' [27].

2.5 Timeliness of the research: our research is especially timely, given the current regulatory, consumer and business environment. Businesses operating in the EU had been subject to GDPR only for four months at the time of our round table sessions; while discussions around an updated E-Privacy Regulation which will impact IoT service providers in the EU were ongoing at the time of the workshops. At the same time, within six months before our round table sessions, the Facebook-Cambridge Analytica scandal, in which the profiles of 87 million primarily US-based citizens were harvested from Facebook without consent by UK-based data analytics firm Cambridge Analytica, and may have been used to influence important political results such as the Brexit referendum [28], was prominent in the news media and has resulted in a heightened consumer awareness of privacy issues and the illicit use of personal data. Our discussions took place at the time at when the UK Information Commissioner's Office (ICO) found *'that the personal information of at least one million UK users was among the harvested data and consequently put at risk of further misuse'* [29] and in October 2018, just after the research team ran the workshops discussed in this paper, ICO levied Facebook the maximum possible fine of £500,000. The scandal had a serious impact on both Facebook and Cambridge Analytica; the hashtag #deletefacebook gained traction in the wake of the scandal [30] and Cambridge Analytica subsequently began insolvency proceedings in the US and UK [31].

3 Methodology

3.1 Study participants: 32 volunteers attended the round-table sessions in partnership with Digital Catapult, an independent 'lab for business' funded partly by the UK government which aims to support data-driven businesses to maximise their contribution to the UK economy. Digital Catapult provided access to its experts, facilities and assistance in advertising the workshops (see Acknowledgements). The sessions were advertised as being of interest to participants from industry, SMEs, policy organisations or consultancies. Participants represented a diverse range of stakeholders in multiple sectors including IoT membership organisations, hardware manufacturers, end-user businesses (utilities, rail, retail, direct marketing), law firms, consultancies, consumer rights groups, marketing and policy organisations, and academics. Participants represented primarily UK businesses but were also from the EU and overseas. There was a representative mix of genders at the sessions.

3.2 Study design: the round-table sessions were advertised through the Digital Catapult website https://www.digicatapult.org.uk and event website EventBrite. The workshops were described as focused on 'The Value of Personal Data in IoT' during which participants would discuss the implications of consumer perspectives on the value of personal data for IoT businesses and consumers themselves, in partnership with Digital Catapult, the University of Warwick, University of Bristol and University of Birmingham (see Acknowledgements). Three round-table sessions were held in London, UK, on 17 and 21 September and 3 October 2018, hosted by Digital Catapult at its offices in King's Cross. The sessions were each attended by a member of the project

advisory board (see Acknowledgements) and the research team, and chaired by a member of the research team. A series of questions were posed by the session chair from a script, as a prompt for an open discussion. The discussion was encouraged to be broad-ranging, enabling participants to raise the issues of greatest interest and importance to them. The discussions were recorded by a note-taker; verbal consent was obtained from participants for their comments to be recorded and used anonymously for publications.

3.3 Thematic analysis: A professional note-taker was employed to make a record of each meeting. It was decided to use a note-taker rather than to record the sessions to enable participants to express their opinions freely. The comments were recorded to preserve the context and meaning of the discussion but not intended to be verbatim quotes. The notes of the sessions were thematically analysed using the methodology proposed by Braun and Clarke [32]. An initial set of over twenty themes was identified and these were iteratively aggregated and refined into three 'analytic' themes, supported by participant comments. These themes are reported on below. Discussion points relating to issues which were not related to consumer conceptions of value of IoT personal data were excluded, for example the use of personal data to monitor personnel in the workplace.

Three overarching, cross-cutting analytic themes were identified, reflecting points of convergence and divergence between industry representatives and consumers, as understood from the industry point of view, a perspective which has been given little attention in previous literature. In support of the three analytic themes, we wish to highlight eight IoT data themes that emerged from the discussion, around the unique and dynamic socio-technical, commercial and regulatory environment that IoT businesses and consumers find themselves in.

4 Results

In this section, participant quotes are provided anonymously, with the participant number denoted by P*X* and workshop denoted by W*Y*. Participant quotes are presented in italics.

4.1 Analytic Themes

4.1.1 Asymmetry of information between industry and consumers: we observed perception of asymmetry of information between well-informed industry 'cognoscenti' and comparatively naive consumers, who have a perceived lack of understanding of the ways in which IoT data companies use their personal data and of the complex legal environment which governs it.

This perceived imbalance was quite general, although participants also referred to differing profiles of consumers which is similar to discussed in the literature [9, 33]: some consumers are better informed and more data-aware than others.

P3W1: *'[There is a] difference between what people who work in the area understand to what other people understand. People who are not in this industry would be aware of the data held on their FitBit for example but less so about what is shared across the internet.'*

P1W2: *'There is a huge amount of misunderstanding in the public about what data can say … Historically we have had transactional services that we have understood, but now it's more systemic, data capturing a multitude of things about me which I don't know. It is sophisticated … We need to go up a level from saying "it's data" and say "What does this data say [about me]". That it what we [industry] are trading and people are at a massive disadvantage from not understanding that.'*

For instance, consumers may view customer loyalty card data or electricity use data as not important or valuable - whereas in fact it can be used to predict risk of future health conditions and therefore could have considerable value to health providers or insurance companies:

One participant mentioned her incredulity that consumers would share so much sensitive information about their health with IoT companies:

P1W3: *'We have seen people willingly share information on emotions, sleep patterns and heart rhythms for example.'*

Such a lack of understanding of the complex environment leaves consumers vulnerable to exploitation, and industry participants stressed the need for better education so that consumers could make better informed choices about sharing their personal data.

P2W1: *'If we are discussing all these issues deeply and the public doesn't understand even at a basic level, how do we bring them to a solution? I think there's lots to do in educating the public.'*

4.1.2 Imbalance of power and the potential for inequality: industry participants felt that the asymmetry of information in the complex IoT personal data environment could lead to an imbalance of power in favour of industry and to the detriment of consumers, with companies increasingly mediating the digital world on behalf of consumers:

P2W2: *'The more data we can collect from you, we get clouds of individual data points and out of that cloud comes Alexa to make sense of that complicated world for you. But also some organisations are putting themselves forward to be that kind of actor on your behalf. These personal assistants will be increasingly mediating our relationship with the world … It needs a higher level of discussion on the social contract between us and institutions [that hold personal data]. It all comes down to ethics, values, what our rights and responsibilities are to each other.'*

It was felt that this imbalance of power could lead to inequalities between different groups of consumers, such as the informed versus naive, wealthy versus poor. One potential

inequality mentioned was that of the undermining of privacy as a right afforded to everyone irrespective of socio-economic group:

P3W3: *'I think the new luxury will be complete privacy and [the ability] to pay for complete detachment from all the electronics and so on.'*

P4W3: *'The issue of paying to protect privacy: There could almost be a 'social' class and a 'privacy' class. Those people who are at the bottom of the strata who are not able to afford to protect it.'*

Others referred to the potential for stratification of value, with personal data from higher socio-economic groups being valued more highly than others, or the potential for price discrimination:

P1W3: *'Some people's data will be of more value than others. So there is going to be price discrimination too. "My data is more valuable than yours".'*

Participants mentioned that the availability of personal data markets might drive vulnerable consumers to sell their personal data for monetary reward despite the risks of sharing:

P5W3: *'Vulnerability is the big concern. Because some people will just share data for money and they might forgo the risks of sharing it.'*

Another comment illustrated a lack of industry understanding of the complexity that consumers must overcome when faced with a choice whether or not to accept the terms and conditions and use an IoT data-driven service, which may extend to contracts which involve data sharing with over 1,000 companies [12]:

P3W3: *'There could be simplicity in the way it [privacy in IoT] is explained. Everyone does have time to read a few words if they are interested'.*

4.1.3 Need for consumer education, greater transparency and control leading to enhanced trust: industry participants understood that consumer trust was fundamental to successful business performance in the IoT, but said they struggled to see how this trust could be achieved, given the complexity of the regulatory and technical environment in IoT, and the confidential nature of personal data processing and algorithms used by IoT companies, even following the implementation of GDPR:

P1W1: *'How do you [consumers] know they [IoT organisations] have to follow the rules?'*

Participants felt that consumer education, transparency and communication of personal data practices to consumers were critical to building trust and therefore further data sharing, which was considered essential in IoT:

P6W3: *'As an organisation [involved in personal data use] it is about building trust otherwise people won't share data. But many people say they have no idea what is going on in terms of data sharing [in IoT]. So transparency and being able to explain is important otherwise they won't share.'*

But this presented a tension as consumer education was a considerable challenge due to the complexity of the environment:

P6W3: *'Presenting the complexity of the business relationships and data transactions, and conveying that to users in a clear, transparent but not overwhelming way or expecting them to become super experts [is difficult]. It's about how you communicate that value exchange to the consumer in a fair and effective manner. How you give them actual control, because people feel they have lost control.'*

Participants felt that IoT companies should take a responsible, ethical stance towards their personal data practices, which would go further than legislative and regulatory frameworks:

P2W2: *'IoT presents a whole new way of thinking about [the relationship between] ourselves and institutions. Our lives are being revealed in even greater intimacy, which gives us power to make better choices but also reveals the minutae of ourselves through institutions.'*

Participants acknowledged that consumers might demand trust from technology, but trust must be driven by the organisations that provide that technology:

P2W2: *'The data world is revealing the nuances of relationships between government, the private sector and individuals. I don't think trust is something you can demand from a technology solution. What you can pin down from that is: Are you [the organisation] trustworthy?'*

4.2 IoT data themes

Eight themes emerged around the unique characteristics of the socio-technical, regulatory and commercial environment surrounding IoT that provide context, rationale and support to the analytic themes.

4.2.1. IoT data have unique characteristics: they are deployed at vast scale, they may incorporate a mix of personal and non-personal data, including location and context-aware, capture data 'passively', i.e. without the input or perhaps awareness of the consumer (for example, the step count measured by a fitness tracker wearable) [10-12]. These characteristics lead to greater complexity and may push consumers 'out of the loop'. The also enable personal data to be linked with non-personal data augmenting the information within and economic value of the data. This creates a disparity between consumer and industry understanding (our first analytic theme) and a loss of trust, transparency and control (third analytic theme), a finding broadly consistent with recent literature [34].

P3W1: *'There is an interesting division between what is IoT data and what is personal data. The banking transaction data starts not as IoT, but if you are interacting with the bank data on mobile devices it does become IoT . ... There is data that you have deliberately created but also there is data about a person passing through IoT fields going down a street. I think you are very concerned with the deliberately created data but the other background to this is all the passive sensing of people that people are even less aware of.'*

P1W1: *'Smart parking devices. They do not in themselves create personal data but if you are able to link them to someone in a car going to a parking space then they create personal data'.*

4.2.2. IoT data have complex supply chains: participants talked about the complexity of managing data sharing across IoT supply chains with multiple actors and ensuring that partners followed the same privacy policies or rules:

P1W1: *'IoT is all about partnerships ... there are 30 or 40 different companies for example that [participant] works for, so how do you know that they manage data to the same standard as you? ... if you have a subscription to a phone, it's managed through a SIM card [and so you know who the provider is]. If you have a sensor in an electricity meter, who should have access to that information? It might not just be the electricity company, aggregated information might be available to another subsidiary.'*

This complex web of third-party arrangements could lead to a loss of control as third-party data sharing agreements may not be easily visible to consumers:

P4W1: *'[Retailer] has a high trust brand yet as a consumer you can end up with your data all over the place because of their interaction with other companies. So there is no control necessarily in lots of cases.'*

4.2.3. IoT enables data to be turned into valuable information through linking and use of algorithms, often without the full knowledge of consumers: industry participants perceive that consumers are only partially aware of the full extent of the manner in which their data drives value for IoT organisations. Participants acknowledged that this mining of data to create new knowledge and information can be much more invasive of privacy than the original data itself, as suggested in [8] and [34]. Industry participants acknowledged that some consumers may not be aware of the sophistication of the algorithmic methods being used to mine their personal data, and that this could have profound consequences:

P3W1: *'How you might find out about a profile crosses through many types of data. People [industry] can be very clever in a way that the consumer might not twig.'*

P3W3: *'I think privacy decreases [due to IoT]. People collecting multiple databases - you can lay on top of that all this location and time, all kinds of data. ... what strikes me is that our privacy is going to diminish as more data is available. So we might end up in a situation like the Chinese one that has social scores of people'* (referring to the proposed social credit system in China widely reported in the press in spring of 2018, discussed for example in [35]).

Others echoed concerns consistent with previous literature [24, 34] of a sense of inevitability, in this case that technology would be used to re-identify people from anonymous data:

P7W3: *'Anonymised data becomes no longer anonymised - technology will soon catch up'.*

4.2.4 Context and purpose are important for consumer conceptions of value in IoT: this observation is not new; the principle that personal data may be used lawfully only for the purposes for which they were collected, was enshrined in UK law and EU regulation prior to the introduction of GDPR and embedded within GDPR. However, the large scale, dynamic nature, supply chain complexity, capacity to link with non-personal data and provide further context stipulates a further risk to privacy and a potential loss of trust, transparency and control by consumers.

P4W2: *'We found people were more happy to share data for the public good. For example in genomics, if they thought it was moving on medical science or in some instances with local government if they thought their services would improve, but not with the private sector to make money.'*

One participant suggested that consumers may only be aware of IoT personal data collection at some point quite far downstream from the origination of the data collection:

P7W1: *'It's when decisions are made, like getting insurance quotes. That's the only time when people understand the purposes [of data collection].'*

4.2.5 Consumer understanding of security in IoT devices: much has been written in previous literature about vulnerabilities and the need for greater security in the IoT [36] and cybersecurity more broadly [37]. Participants agreed that there was an urgent need for consumer education on the topic.

4.2.6 Personal data underpins business models in the IoT:. industry participants provided many examples of personal data underpinning IoT business models, such as tracking driving behaviour by insurance companies to reduce insurance premia, monitoring energy usage to promote efficiency, fitness tracking to promote health or monitoring movement in the home to support elderly relatives - these examples corroborate the literature: e.g. [4], [11], [12]. Participants viewed these business models in general as a positive and beneficial for consumers, whilst recognising that consumers may not necessarily understand the range of uses to which their data might be put. We return to this point in the discussion.

4.2.7 Changes in business practices arising from GDPR: from the discussion arising in our workshops, it seems that business practices are changing in the IoT industry in favour of consumers as a result of GDPR - for example, the introduction

of summary privacy policies, data collection with a clear purpose and restrictions around data transfer out of the European Economic Area:

P3W3: *'Everyone* [business] *was being encouraged to have a 'data play'. People were collecting information without any idea of what to do with it. They said at some point 'This is the new oil' but we called it uranium because it can be of value or it can be really deadly ... I think the good part of GDPR is the blockage of no purpose collection of data.'*

Participants acknowledged the implementation of GDPR as a generally positive change in favour of consumers, but said that simplicity for consumers was challenging to achieve given the complexity of the regulation:

P5W2: *'GDPR is trying to get us to that point [where privacy policies are easy to understand]. I am sceptical about how effective that is for people. Google for example have their privacy page and you can see it but it's quite complicated. There's a paradox within GDPR: You have to tell people this information, but you have to do it in a simple, concise way and I honestly don't think that's possible. I don't think you can give all the information you need to in a nice easy way'.*

Although we heard examples of business practice changes in the IoT as a result of GDPR, as predicted and discussed in previous literature [38], at the time of the workshops, there was little evidence of new business models or innovation arising from GDPR. Personal data stores were discussed as a potential method of value generation by new businesses and enhanced control by the user, but there were differing views expressed of how successful they had been to date or might be in future.

4.2.8 A need for debate around personal data ownership, rights and responsibilities: industry participants stated that there was confusion amongst consumers and industry professionals themselves around the legal regime surrounding ownership of personal data and the rights and responsibilities of data subjects, data controllers and data processors. Participants acknowledged that consumers view themselves as data 'owners', but that in terms of the European Intellectual Property Framework, personal data cannot be owned as it is a fact and therefore does not attract intellectual property rights. Some participants felt that consumers should have the right to 'own' their personal data, while others disagreed and felt that a system of rights of data subjects and responsibilities of data controllers or processors was more appropriate. This topic is the focus of recent analysis [39] and an open research challenge. One participant suggested that the framework proposed by Abrams [40] for modes of personal data collection - Provided, Observed, Inferred, Derived - could provide a useful framework for understanding these rights and responsibilities.

P4W2: *'There is obviously a huge shift [needed] in the way that people think about personal data. The ownership of data has to rest with individuals. The idea that I have to pay people to protect my data is not good. It's my right [to own my personal data] and it's my right [even] if I give you my data for you to protect it. I think there is a massive learning [required by industry] on that.'*

P4W3: *'The ability to sell data - we probably should not [be able to do that] because there is no ownership.'*

Issues were raised of the complexity of personal data about more than one person, where rights might be shared, for example in the context of social media:

P6W1: *'It relates to who owns the data. There is data that I created about myself on social media but at what point is it my data or someone else's?'*

Another scenario articulated was where information on one individual might inadvertently reveal information on another, such as in family groups:

P6W2: *'In terms of data ownership and ethics, most data is about more than one person. For example, DNA reveals things about your parents and family. So how we are operational with that is a big question.'*

5 Discussion

Our research was intended to elucidate perspectives from industry stakeholders of consumers' knowledge, preferences and behaviour regarding their personal data in IoT, and in particular their conceptions of value in terms of risks and benefits. We identified three overarching analytic themes supported by IoT data themes which arise from the complex socio-technical, commercial and regulatory environment surrounding IoT businesses. Industry participants identified an asymmetry of information between industry and consumers, leading to a perceived imbalance of power and the potential for inequalities. Industry participants stated that greater transparency of personal data practices and enhanced consumer control would lead to greater trust and enhanced business value, but this was dependent on consumer education and empowerment.

Information asymmetry between industry and consumers with respect to privacy is a key theme identified in previous literature [8, 24] but has not been fully explored in the context of IoT businesses. Acquisti et al [8] observed that *'consumers are rarely (if ever) completely aware about privacy threats and the consequences of sharing and protecting their personal information. Hence, market interactions involving personal data often take place in the absence of individuals' fully informed consent.*'

We found the degree of divergence between industry and consumer understanding of IoT personal data practices surprising, although the consumer perceptions would need to be further tested as our roundtable discussions explored the views of consumers as perceived by industry. Although, in general, industry participants were concerned about information asymmetry, they had a tendency to underestimate the complexity of the environment for consumers - for example, stating that everyone had time to read a privacy

policy, whereas privacy contracts are only fully transparent once third-party sharing and data processing agreements are understood [24]. Such documents are rarely made available to consumers and the scale of the task required to understand them maybe be prohibitive.

Industry participants identified that this asymmetry of information led to an imbalance of power between IoT businesses and consumers, that could have profound ethical consequences: such as companies placing themselves as mediators of the digital world on behalf of consumers. Industry participants identified other ethical consequences of IoT data sharing: the potential for price discrimination based on socio-economic status; inequalities between different socio-economic groups; the exploitation of vulnerable consumers, such as children; and consumers being incentivised to take unacceptable levels of risk from selling their data for monetary reward. Aspects of these themes have been considered previously in the literature - for example, the UK Competition and Markets Authority published a report about the commercial use of consumer data in 2015 [42] and recently announced new research into price discrimination in e-commerce [43]. Previous research has considered consumer perceptions of fairness of privacy [44], however the idea of a socio-economic inequality based on privacy (those who can afford to pay for privacy and those who cannot, and therefore whose data is available for mining) was surprising.

Industry participants felt it was incumbent upon them to educate consumers about what might happen with their personal data and explain the risks and benefits more clearly, but that this was considered a considerable challenge given the complexity of the environment, compounded by the commercial confidentiality surrounding algorithmic processing of personal data, which many organisations regard as competitive capabilities to be protected as trade secrets. Participants struggled with the contradiction of wanting to help consumers make informed choices but being hampered by the inherent complexity of the environment, and the tension between legal, ethical and commercial concerns. Industry representatives talked about the ethical and moral responsibilities of companies, but acknowledged that the industry lacks an ethical code of practice beyond the legal confines of GDPR.

A number of other themes are worthy of note. The complexity of IoT supply chains has been noted in the literature [36] but the impact on consumer transparency of personal data practices, perhaps less so. Each player in the supply chain has data processing and data transfer agreements with other players which may not be transparent to consumers. Companies generally include terms in their contracts which state that they are not responsible for the data practices of others, but that allow for data to be transferred to other entities. In Europe, the introduction of GDPR confers 'joint and several' responsibility for data sharing between data controllers under certain circumstances (joint controllership applies if two or more companies jointly determine the purposes and means for the processing of personal data under Article 26) but it will probably take a significant IoT breach for the new liability to be tested. The lack of consensus around whether consumers should have 'ownership' of personal data was also intriguing, an issue explored in recent research by Janeček 2018 [39]. An interesting avenue for further research would be to investigate whether rights of ownership of data beyond rights of access and responsibilities of controllers and processors would confer more control or transparency in the minds of consumers, or better practices by industry.

One participant mentioned the taxonomy proposed by Abrams [40] as a useful framework for understanding personal data collection based on the manner in which data originates - Provided, Observed, Inferred, Derived. This framework was adopted by the influential European Commission Article 29 Data Protection Working Party (now superseded by the European Data Protection Board) in its guidelines for data portability. It is interesting to note that this guidance considers 'provided' and 'observed' data to be subject to data portability rights, but not inferred or derived data [41]. Such an interpretation of data portability is pragmatic but could unwittingly compound the imbalance of power we observed between industry and consumers, because in IoT data are 'not collected directly from the individual but, rather, at a distance without the individual's awareness of its origination and subsequent uses' [40].

Our research revealed a perception within industry of significant differences between industry and consumers in the understanding of what personal data is, who owns it, how it is used in IoT products and how it drives value in IoT businesses. Our research was conducted with a small sample size of 32 participants and provides a snapshot of views from a diverse panel of industry representatives, but is far from conclusive. It gives an insight into the range of views around personal data sharing in IoT and has implications for business practices, governance and regulation, with which we conclude below.

6 Implications: Towards a Manifesto for Personal Data in IoT

Here we present a tentative five-point manifesto for personal data in IoT, as a response to correct the asymmetry of information between industry and consumers; to redress the perceived imbalance of power; to reduce the potential for inequalities; and to enhance the transparency of personal data business practices by IoT businesses in favour of consumers, increasing trust and overall business value. While this would need broad consultation with industry stakeholders and policy-makers, we hope that it will form a basis for future research and discussion.

6.1 Consumer education campaign: industry stakeholders could work with consumer groups such as Which? and the Information Commissioner's Office in the UK to develop a consumer education campaign on the risks and benefits of personal data collection and use in IoT. This campaign should be high-profile, in order to reach a broad cross-section of consumer groups, accessible, in plain English and could include case studies which explain in detail how personal data is used in IoT businesses, a topic which is often kept

confidential by companies. The campaign could provide vignettes explaining how seemingly 'innocent' types of personal data - like electricity use, loyalty cards data and physical activity records- can be used to infer health, financial status and other sensitive personal information.

6.2 IoT personal data ethical practice guidelines: industry stakeholders could work collectively through IoT membership organisations, trade groups and the recently-established Ada Lovelace Institute and Centre for Data Ethics and Innovation in the UK, to establish guidelines for ethical personal data practices in IoT which go beyond the minimum standards imposed by GDPR. These could include determining better transparency of third-party personal data processing arrangements, more fundamental explanations of algorithmic decision-making that are accessible by and understandable to consumers, or exploring the ethical consequences of new business models such as privacy-as-a-service.

6.3 A trustmark, standards or codes of practice to supplement regulation in specific domains: following on from the recent suggestion for a statutory code of practice for personal data use in political campaigns, we suggest that the IoT industry could consider establishing a trustmark, industry-wide standards or voluntary/statutory codes of practice for specific areas of sensitive personal data use in IoT, such as location data, health data or biometric data. Such standards could give consumers confidence that they are using products and services with responsible personal data practices and give businesses a competitive edge.

6.4 IoT personal data 'accounts': there is a need for continued scrutiny of personal data practices in IoT businesses, both to enhance the trust and value in responsible IoT businesses and also to ensure that consumers are protected from potential irresponsible practices. Building on the principle of voluntary disclosure (for e.g. the gender pay gap or corporate social responsibility), one way of achieving this might be for IoT companies to voluntarily publish personal data 'accounts'. Such accounts could voluntarily disclose information on personal data practices such as third-party processing agreements, transfers outside the European Economic Area, subject access requests or deletions based on the 'right to be forgotten'.

6.5 Further research into personal data ethics and impact on consumer groups: policy-makers, consumer rights groups, regulators and researchers should investigate ethical issues arising from inequalities in personal data practices in the IoT, for example the potential for privacy protection to be available only to the wealthy, discriminatory pricing based on socio-economic status; and implications for vulnerable groups of consumers, such as teenagers and older people. Further research should be conducted into the perspectives of consumers of the issues raised.

7 Conclusions

Three key overarching analytic themes emerged through our workshops exploring industry perspectives of consumer conceptions of the value of personal data in IoT, informed by eight 'IoT data' themes which are characteristic of the unique socio-technical, regulatory and commercial environment faced by IoT businesses. First, the discussion revealed an information asymmetry between industry and consumers around the risks and benefits of personal data in IoT, which manifested itself as perceived disparities in understanding over key issues such as personal data collection and use, the rights of consumers and responsibilities of industry. Second, industry participants highlighted the potential for this asymmetry to cause an imbalance of power between industry and consumers, and inequalities between different consumer groups. Third, our research highlights a need for consumer education and greater transparency around the use of personal data in IoT and the ways in which it drives value for businesses, in order to enhance transparency, trust and business value. Finally, we presented a tentative five-point manifesto for personal data in IoT to redress the balance. Further research and engagement between stakeholders is required to ensure fairness, value and accountability for consumers; and an ethical, innovative, competitive future for IoT businesses.

8 Acknowledgements

The authors acknowledge the main funder of the Value of Personal Data in IoT project to be the UK Hub for Cyber Security of the Internet of Things, PETRAS, under the EPSRC grant EP/N02334X/1.

The authors acknowledge funding and support of Digital Catapult, https://www.digicatapult.org.uk/, an independent 'lab for business' funded by the UK government through UK Research and Innovation, which aims to support data-driven businesses to maximise their contribution to the UK economy. Digital Catapult funded the costs of an independent researcher, Lucie Burgess, of Helix Data Innovation, to contribute to the Value of Personal Data in IoT study.

The authors would like to thank the project Advisory Board for their contributions to the project and during the round table sessions: James Edgar, Head of Policy, Digitisation/ Energy at Which?; Guy Johnson, Data Protection Officer and Head of Data Governance, Marks and Spencer; Dr Kenji Takeda, Director, Azure for Research, Microsoft; Graham Trickey, Head of IoT, GSM Association; and Dr Alex Gluhak, Head of Technology (IoT), Digital Catapult.

9 References

[1] Maple C.: 'Security and privacy in the Internet of Things', Journal of Cyber Policy, 2017, 2, (2), pp. 155-184

[2] 'IoT Analytics: State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating', https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/, accessed 25 February 2019

[3] Digital Catapult internal estimate, unpublished.

[4] Perera C., Liu C. H., Jayawardena S.:'The emerging internet of things marketplace from an industrial perspective: A survey', IEEE Transactions on Emerging Topics in Computing, 2015, 3, (4), pp. 585-598

[5] 'IDC - Worldwide Internet of Things Survey 2017-2021', https://www.idc.com/getdoc.jsp?containerId=US43087717, accessed 25 February 2019

[6] 'Transparency Market Research - Data broker market, global industry analysis, size, share, growth, trends and forecast 2017 – 2026', https://www.transparencymarketresearch.com/data-brokers-market.html, accessed 25 February 2019

[7] 'European Commission and IDC - The European data market final report: Study dataset', http://datalandscape.eu/study-reports, accessed 25 February 2019

[8] Acquisti, A., Taylor, C., Wagman, L.: 'The economics of privacy', Journal of Economic Literature, 2016, 54, (2), pp. 442-92

[9] *Which?*, 'Control, Alt or Delete? Consumer research on attitudes to data collection and use' (2018), pp. 1-91

[10] Atzori, L., Iera, A., Morabito, G.: 'The internet of things: a survey. Computer Networks, 2010, 54, pp. 2787–2805

[11] Li, S., Xu, L.D., Zhao, S.: 'The internet of things: a survey'. Information Systems Frontiers, 2015, 17, (2), pp 243–259

[12] Mishra, D., Gunasekaran, A., Childe, S.J., Papadopoulos, T., Dubey, R., Wamba, S.: 'Vision, applications and future challenges of internet of things: a bibliometric study of the recent literature'. Industrial Management and Data Systems, 2016, 116, (7), pp 1331–1355

[13] Shin, D. H.: 'Conceptualizing and measuring quality of experience of the internet of things: Exploring how quality is perceived by users', Information & Management, 2017, 54, (8), pp 998-1011

[14] Hsu, C. L., Lin, J. C. C.: 'An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives', Computers in Human Behavior, 2016, 62, pp 516-527

[15] Chang, Y., Dong, X., Sun, W.: 'Influence of characteristics of the internet of things on consumer purchase intention', Social Behaviour and Personality: an International Journal, 2014, 42, (2), pp 321–330

[16] Malhotra, N., Kim, S., Agarwal, J.: 'Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model', Information Systems Research, 2004, 15, (4), pp. 336-355

[17] Barnes, S. B.: 'A privacy paradox: social networking in the United States', First Monday, 2006, 11, (9)

[18] Taddicken M.: 'The 'privacy paradox'in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure', Journal of Computer-Mediated Communication, 2014, 19, (2), pp. 248-273

[19] Blank G., Bolsover G., Dubois E.: 'A new privacy paradox: Young people and privacy on social network sites'. Prepared for the Annual Meeting of the American Sociological Association, 2014, 17, pp. 1-34

[20] Yang Y., Wu L., Yin G., et al.: 'A survey on security and privacy issues in Internet-of-Things,' IEEE Internet of Things Journal, 2017, 4, (5), pp. 1250-1258

[21] Zhou, W., Piramuthu, S.: 'Information relevance model of customized privacy for IoT'. Journal of Business Ethics, 2015, 131, pp 19–30

[22] Kim, D., Park, K., Park, Y., Ahn, H.: 'Willingness to provide personal information: Perspective of privacy calculus in IoT services', Computers in Human Behavior, 2019, 92, pp 273-281

[23] Lu, Y., Papagiannidis, S., Alamanos, E.: 'Internet of Things: A systematic review of the business literature from the user and organisational perspectives', Technological Forecasting and Social Change, 2018, 136, pp 285-297

[24] Zuboff, S.: 'Big other: surveillance capitalism and the prospects of an information civilization,' Journal of Information Technology, 2015, 30(1), pp. 75–89

[25] 'Mozilla:10 Fascinating Things We Learned When We Asked The World 'How Connected Are You?'' https://blog.mozilla.org/blog/2017/11/01/10-fascinating-things-we-learned-when-we-asked-the-world-how-connected-are-you/, accessed 25 February 2019

[26] Deloitte Research, 'Switch on to the connected home' (2016), pp.1-24

[27] Tsai, J. Y., Egelman, S., Cranor, L., Acquisti, A.: 'The effect of online privacy information on purchasing behavior: An experimental study', Information Systems Research, 2011, 22, (2), pp. 254-268

[28] Information Commissioner's Office, 'Investigation into the Use of Data Analytics In Political Campaigns: a report to Parliament' (2016), pp. 1-116

[29] 'The Guardian - ICO issues maximum £500,000 fine to Facebook for failing to protect users' personal information',

https://www.theguardian.com/technology/2018/oct/25/facebook-fined-uk-privacy-access-user-data-cambridge-analytica, accessed 25 February 2019

[30] 'Evening Standard - #DeleteFacebook: Scores of people vow to shut down accounts after Cambridge Analytica data leak,https://www.standard.co.uk/news/uk/delete-facebook-scores-of-people-vow-to-shut-down-their-accounts-after-cambridge-analytica-data-leak-a3794256.html, accessed 25 February 2019

[31] 'The Guardian - Cambridge Analytica closing after Facebook data harvesting scandal', https://www.theguardian.com/uk-news/2018/may/02/cambridge-analytica-closing-down-after-facebook-row-reports-say, accessed 25 February 2019

[32] Braun V., Clarke, V., 'Using thematic analysis in psychology', Qual. Res. Psychol., 2006, 3, (2), pp. 77–101

[33] 'Open Data Institute - ODI survey reveals British consumer attitudes to sharing personal data', https://theodi.org/article/odi-survey-reveals-british-consumer-attitudes-to-sharing-personal-data/, accessed 25 February 2019

[34] Wachter, S.: 'Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR', Computer Law & Security Review, 2018, 34, (3), pp 436-449

[35] Liang, F., Das, V., Kostyuk, N., Hussain, M. M.: 'Constructing a data-driven society: China's social credit system as a state surveillance infrastructure', Policy & Internet, 2018, 10, (4), pp. 415–453

[36] Adams, M.: 'Big Data and individual privacy in the age of the Internet of Things', Technology Innovation Management Review, 2017, 7 (4), pp. 2–24.

[37] Coventry, L., Briggs, P., Blythe, J., & Tran, M. 'Using behavioural insights to improve the public's use of cyber security best practices' (UK Government research report, 2014).

[38] Tikkinen-Piri, C., Rohunen, A., Markkula, J.: 'EU General Data Protection Regulation: Changes and implications for personal data collecting companies', Computer Law & Security Review, 2018, 34, (1), pp 134-153.

[39] Janeček, V.: 'Ownership of personal data in the Internet of Things', Computer Law & Security Review, 2018, 34, (5), pp 1039-1052

[40] Abrams, M.: 'The origins of personal data and its implications for governance' (The Information Accountability Foundation, 2014), pp. 1-12

[41] European Commission Article 29 Data Protection Working Party, 'European Commission Guidelines on the Right to Data Portability' (European Commission, 2016).

[42] CMA, 'The commercial use of consumer data: research report' (DotEcon and Analysys Mason, 2015), pp. 1-163

[43] 'GOV.UK - Government and CMA to research targeting of consumers through personalised pricing', https://www.gov.uk/government/news/government-and-cma-to-research-targeting-of-consumers-through-personalised-pricing, accessed 25 February 2019

[44] Krishen, A. S., Raschke, R. L., Close, A. G., Kachroo, P.: 'A power-responsibility equilibrium framework for fairness: Understanding consumers' implicit privacy concerns for location-based services', Journal of Business Research, 2017, 73, pp. 20-29