The IoT and Unpacking the Heffalump's Trunk

Joseph Lindley, Paul Coulton, Rachel Cooper

Imagination, Lancaster University, United Kingdom
{j.lindley|p.coulton|r.cooper}@lancaster.ac.uk

Abstract. In this paper we highlight design challenges that the Internet of Things (IoT) poses in relation to two of the guiding design paradigms of our time; Privacy by Design (PbD) and Human Centered Design (HCD). The terms IoT, PbD, and HCD are both *suitcase terms*, meaning that they have a variety of meanings packed within them. Depending on how the practices behind the terms are applied, notwithstanding their well-considered foundations, intentions, and theory, we explore how PbD and HCD can, if not considered carefully, become *Heffalump traps* and hence act in opposition to the very challenges they seek to address. In response to this assertion we introduce Object Oriented Ontology (OOO) and experiment with its theoretical framing order to articulate possible strategies for mitigating these challenges when designing for the Internet of Things.

Keywords: Internet of Things, Privacy by Design, Human-Centered Design

1 Introduction

Although the term the Internet of Things (IoT) is employed regularly, particular in discussions relating to emerging technologies, its actual meaning is ambiguous as it is defined differently depending on who's using it and in what context. Although it was preceded by other terms such as ubiquitous computing and pervasive computing it has gained traction with a general audience, perhaps because the terms 'internet' and 'things' are more accessible. However, having ambiguity baked in to the term means that 'the IoT' is likely to be interpreted differently dependent upon the meanings a particular individual might associate with these terms. This ambiguity means there is huge variation within discourses utilizing the term. Although the research presented in this paper is aimed at contributing to practices relating to the design of IoT products and services, it also resonates with other, more general, discussions relating to emerging technologies. In particular it seeks to contribute to the debates about privacy, ethics, trust and security in the IoT [37] and understand potential barriers to adoption that may arise through the establishment of problematic design patterns.

Our title is a play on the word trunk being synonymous with suitcase, and makes reference to Hyman Minsky's term, *suitcase words*. These words describe complex concepts that, when one tries to define them, reveal a nested series' of other meanings contained within. The other odd term in the title, *Heffalump*, refers a fictional elephant like creature, appearing in A.A. Milne's books about *Winne the Pooh*. In one story Pooh

and his friend Piglet decide to catch a Heffalump in a cunning trap, unfortunately they only succeed in trapping *themselves*. The irony of this story has given rise to Heffalump Traps being used by political journalists to describe strategies in which a politician might set a rhetorical trap to catch their opponent and that ultimately backfires on the trapper, leaving them to appear foolish! Thus, despite their intentions, and often fine execution, Heffalump traps fail to achieve their aims and instead are detrimental toward the desired outcome. In this paper we illustrate how the suitcase terms IoT, Privacy by Design (PbD), and Human Centered Design (HCD) can, become Heffalump traps by virtue of their nested complexities.

The paper is structured as follows. First, we discuss PbD, paying particular attention to the linguistic complications when trying to define what it really means using the example of the ambiguity present in the European Union's invocation of the term in the recently introduced (EU) General Data Protection Regulations' (GDPR). Next, we discuss the challenge to the well-established paradigms of Human-Centered Design (HCD) resulting from the complexities introduced by networked nature of IoT products and services. Third we argue that, if interpreted hubristically, PbD and HCD can result in unintended consequences, and, in essence, become Heffalump traps. Finally, we propose the use of new design research techniques incorporating concepts derived contemporary philosophies of technology that can be used to develop and test strategies when navigating the complexities of the IoT and thus to minimize the risk of becoming caught in a Heffalump trap.

2 Privacy by Design (and *This* by *That)*

It is important to start this discussion by acknowledging that PbD does not exist in isolation; there are other propositions which overlap with it such as privacy, security and/or data protection by default. The semantics of the terms use does not aid our understanding; for example, configuring something *by default* would not the same as creating something in a particular way, or put differently, *by design.* Although, for something to have a default configuration implies that it *must* have been designed that way. Adding to this confusion is the fact that in English language the word 'design' can be used in a multitude of different way to mean very different things, e.g. the *designer* uses her/his knowledge of *design* to *design* a thingamajig, which was part of the final system *design* (which was built in accordance with the original *design* schematic). It was perhaps inevitable for confusion to result when the terms appeared in an influential report in the form "incorporates *Privacy by Design* principles by default" [6].

The already murky waters that contain PbD are made more difficult to navigate when we introduce the complex abstractions like 'privacy' and 'security'. To unpack these very quickly: privacy is not the same as security, but in some circumstances, privacy may be delivered *by* security and conversely security may be delivered *by* privacy. It is also evident that disciplinary idiosyncrasies can also come into play when trying to bring some clarity to a particular situation. For example, an engineer may interpret *security* operationally in terms of a particular implementation, like access control lists, whereas a psychologist may draw their understanding from a psychological theory, such as Maslow's hierarchy of needs. While both considerations are equally valid even when their epistemological roads intersect, a common understanding will not necessary

emerge. These definitional complexities are not, in themselves, anything to do with how one delivers PbD, they must be acknowledged within any critical discussion. Whilst the argument in this research is relevant to wider discourses of emerging technology, primarily the *specific* issues we are concerned with are (1) *Privacy by Design* [6] and (2) *Data protection by design and by default* as referred to in article 25 of the GDPR [42].

Whilst the term PbD emerged originally in a 1995 report[1] it came to prominence in 2012 through the work of Ann Cavoukian and Jeff Jonas [6]. Introducing PbD Cavoukian quotes the words of a 13th century Persian poet who posits that to 'reinvent the world' one must 'speak a new language'. The premise is that technological progress is itself a new language that brings with it fundamental challenges to the notion of privacy. Going on to provide more concrete examples, the report describes the use of a one-way hash function to protect data subjects' privacy so that even if patterns can be observed in the data, it cannot be reverse engineered to reveal the names of the participants. While this, and the other examples provided are compelling they are arguably a little naïve. Although in particular contexts such approaches can protect the privacy of individuals represented in the data in the increasingly heterogeneous contexts the IoT represents they can be extremely vulnerable to exploitation through amalgamation with other, seemingly unconnected, data sources and complete reliance on them could prove detrimental. In the report Cavoukian builds upon the technical contribution of Jeff Jonas to propose seven principles for the creation of systems that are private by design. These include:

- Full attribution of each data record;
- Data is tethered (any changes to data are recorded at the time of change);
- Analytics only occur when data has been anonymized;
- Tamper-resistant audit can be performed;
- Systems are created that tend towards false negative rather than false positive in borderline cases;
- Self-correcting conclusions (conclusions can be changed based on new data analysis);
- Information flows are transparent (data movements should be trackable and traceable—whether that is through a hard copy, appears on monitor, or is sent to another system)

These principles are aimed at what the report refers to as 'sense making systems', systems that synthesize data from multiple systems such as payroll, customer relationship management, financial accounting, in order to reach new workflow conclusions. While the principles make some sense within the bounded context described, they are regrettably *too* specific to become generally applicable to the heterogeneous user groups and devices founfd within the IoT.

In her discussion of PbD Sarah Spiekermann notes "Data is like water: it flows and ripples in ways that are difficult to predict" [33], the implication being that PbD is rather idealistic and when implemented in practice can be as simple as the utilizing Privacy-Enhancing Technologies with additional security, with the aspiration being an

[1] http://www.ontla.on.ca/library/repository/mon/10000/184530.pdf

apparently "fault-proof" system. Although such an aim is worthy, and the approach is valid, as she states, "the reality is much more challenging". Spiekermann problematizes this idealism by reflecting business models of Google and Facebook. They provide a range of apparently 'free' services but "without personal data such services are unthinkable". She argues that proponents of PbD "hardly embrace these economic facts in their reasoning". In other words, it may not be *possible* to create feature rich systems that are profitable for the companies that supply them without contravening some of PbD's fundamental ideals.

In Cavoukian's response, whilst broadly agreeing with Spiekermann's analysis, she also insists "the challenges of PbD are not as great as Spiekermann suggested; the engineers I have met have embraced the PbD principles, finding implementation not difficult" [5]. Whilst this may be true, it somewhat misses the more interesting element of Spiekermann's analysis which touches on potentially systemic shortcomings at the core of PbD's rhetoric: a 'fault-proof' landscape is unrealistic when the 'economic facts' of many business models are not acknowledged. Spiekermann's critique highlights that to do PbD effectively, it must become part of overall organizational culture, cutting across management, finance, marketing, design and engineering. This is perhaps the reason behind why PbD stagnates, and struggles to move from principles to practicalities—particularly in consumer goods. An alternative perspective on this echoes Shapiro's suggestion that neither engineers nor customers are able to properly articulate, understand, or analyze the impact of 'non-functional' requirements like privacy [32]. These hard-to-grasp requirements operate at a completely different level of abstraction to what either engineers and customers are accustomed to thinking about.

To recap, the new language of technology is making our world anew, but, we are not yet fluent in this emerging language. While purely technical responses to privacy sometimes *appear* to offer faultless solutions (e.g. processing irreversibly hashed data), rarely will such a solution be generalizable across a range of contexts. While principles of PbD appear to be useful mechanisms they can be easily compromised when the complexities of 'in the wild' contexts are encountered. Whilst we are not disputing that PbD has demonstrably helped inform the delivery of privacy-aware projects with buy-in from developers, customers, and management alike, such examples appear to be in very specific contexts and do not necessarily cut through the aforementioned issues. Although the rhetoric deployed for PbD hints at the practicality of creating a 'fault-proof' approach to privacy this fails to appreciate the economic realities of what currently makes data-centric businesses viable.

On the 25th May 2018 when GDPR became active the data protection legislation across a large swathe of Europe immediately changed. As GDPR protects citizens regardless of where the data pertaining to them is being held, it has also impacted on any organization who holds data *about* European citizens. We are yet to fully understand how GDPR will play out in practice, test cases and precedents will need emerge before its full implications are understood. Notwithstanding this uncertainty, GDPR is being cited as a legal framework that will clarify and enforce PbD, because article 25 of GDPR explicitly mentions *Data protection by default and design* [40]. The opening words of the article say that data controllers must take "the state of the art" approaches of PbD into account however no indication is given to what state of the art might mean in practice [14]. Given that this assertion is made under the heading 'data protection by design and default' we might reasonably infer that there is a relationship

between the two, although the *nature* of that relationship is undefined. Article 25 also makes reference to the 'by default' trope, stating that appropriate measures should be taken to ensure that by default "only personal data which are necessary for each specific purpose of the processing are processed". Thus, it appears that GDPR's interpretation of data-protection by design, and relatedly by default, is at best ambiguous and certainly does not progress our understanding of how to effectively operationalize the rather abstract principles of PbD. This lack of specificity with respect to PbD (and its relatives) is not confined to the document defining GDPR. The UK Information Commissioners Office (ICO) which is the UK organization responsible for interpreting and enforcing GDPR calls on data controllers to utilize PbD, but does not proffer any guidance as to how this may be practically enacted[2]. While the definitional challenges facing European regulators are undoubtedly significant, by including the terminology within the text of GDPR without attending to PbD's inherent ambiguity, further challenges are almost certainly abound.

3 Human-Centered Design

In his book *The Design of Everyday Things* [27] Don Norman presented principles for designing 'things' in such a way that human interaction with them is smooth and fruitful. Until relatively recently such interactions tended to occur predominantly between users, things and/or systems that were standalone and self-contained. In the book Norman provides numerous examples including a refrigerator, a telephone, and a clock. Despite the fact that some of his examples, such as the telephone, depend upon several technologies interacting across a diverse technical infrastructure, the user *experience* of using the phone is encapsulated within a discrete interface made up of handset, dialer, and ringer. Today, interactions occur in much more complex contexts which present designers with new challenges. The "networkification of the devices that previously made up our non-Internet world" [29] is creating the IoT and while, interactions with these devices may appear familiar on the surface they inevitably produce an associated digital residue. This digital residue is data, and in stark contrast to the "visibility, appropriate clues, and feedback of one's actions" that Norman highlights as key properties of HCD [27:8–9] the full impact of the data is rarely visible either during or after actual user interactions (with connected, or IoT, devices). While this data is necessary to support business models, to train algorithms and, ultimately, to *make stuff work*, it is possible that by obscuring agency of underlying data, models and algorithms at the point of interaction, designers are in fact operating *against* the underlying ideology of HCD.

The foundations of HCD are in ergonomics with the aim of supporting the "ways in which both hardware and software components of interactive systems can enhance human-system interaction" [43]. Despite being demonstrably useful [2,16] this engineering derived paradigm relied on simplifications of complex contexts [11,13,38]. These reductive stances are incompatible with other more modern approaches that have become integral to HCD and acknowledge "the coherence of action is not adequately explained by either preconceived cognitive schema or institutionalized social norms"

[2] https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/

[36:177]. The result is that HCD methods have become extremely diverse, build upon a variety theoretical and epistemological stances, and are applied variously as both an evaluative and a generative tool [13,23,34]. The spectrum of approaches to utilizing HCD now includes methodological assemblages that can draw upon ethnography, participatory design, cultural probes, workshop techniques, scenarios, extreme users, and personas. Applied sensitively these techniques can produce designs that are "physically, perceptually, cognitively and emotionally intuitive" [13], while also matching "the needs and capabilities of the people for whom they are intended" [27:9]. Whilst it's true that "there is no simple recipe for the design or use of human-centered computing" [17], HCD—particularly among the design research community—has become ubiquitous is greatly influence on the technologies that concurrently we shape, and then ultimately shape us.

Even amongst this diverse methodological landscape, a core theme that pervades HCD utilization is the axiom of simplicity. This is oft interpreted to mean that HCD should inform the design of services and software that are efficient, effortless, and edifying to use; that fade into the background becoming invisible, and that ensure any complexity is that of the underlying task and not of the tool that has been developed to achieve it [25:197,26]. Norman himself acknowledges that dogmatically blunt interpretations of this simplicity axiom can, perhaps unsurprisingly, introduce unintended consequences that drive HCD towards a "limited view of design" and result in analysis preoccupied with narrowly focused "page-by-page" and "screen-by-screen" [24] evaluations. This narrow focus can stifle potential users, and/or *researchers*, form being able to fully intuit a particular designed 'thing' on a crucial cognitive, emotional, and perceptual level. In the hyper-connected and data-mediated assemblages of the IoT, the prevalent assumption that simpler-is-better is already proving highly problematic as the recent revelations concerning Facebooks use of data illustrate. While some aspects of HCD are worthy and hold fast, the complexity, ubiquity, and interconnectedness of *systems*—represented by the IoT—means that HCD needs to be reevaluated. In the age of the IoT, whilst we need to reflect the human centered ideals of HCD, it may be necessary to accept that there are, effectively, multiple centers and actants relevant to any given interaction.

4 Hubris and Heffalumps

The common thread that connects the previous discussions of PbD and HCD relates to the risk that occurs when their principles are interpreted hubristically; with excessive self-confidence. To illustrate this, take a moment to think about the story of the *Titanic*. The ship employed cutting edge technology in an effort to make as safe as possible and was famed for being 'unsinkable'. As well as explaining a lack of lifeboats on board, this inflated confidence meant that even though a spotter saw the iceberg in good time, the helmsman was never asked to take avoiding action—if the ship is unsinkable, why avoid a sinking hazard? After the tragedy the owners were accused of using misleading rhetoric about her sinkability, in response they pointed out their claim was only that the ship was *designed* to be unsinkable (as opposed to *actually being* unsinkable). The tale of the Titanic illustrates that hubristic reliance can, if circumstances conspire, be extremely dangerous.

Relying on supposed guidelines and principles for HCD and PbD is, arguably, equivalent to the Titanic's relying on cutting edge anti-sinking technologies. Hence, we cast HCD and PbD as *potential* Heffalump traps. By solely relying on these approaches—despite their unequivocal worthy aims and demonstrated practical virtues—technologists may inadvertently end up ensnaring themselves by the very issues that HCD or PbD may have sought to avoid (see figure 1). The problem, in many ways, is with binary and didactic positions. Describing ships as unsinkable, systems as private, or designs as human centered—is irrational. The results of such irrational beliefs may, at worst, result in tragedies like the Titanic. The IoT is so pervasive that the scope of resulting impacts range from the relative inconsequence of the Mirai botnet taking down Netflix, through to the destabilization of national infrastructure and potential dissolution of democratic processes.

If treated insensitively, ideals like PbD and HCD may coerce technologists to believe that privacy is something that can be 'achieved' and a system's simplicity is analogous to being 'human centered'. Notions of apparently perfect systems are as dangerous as considering a ship unsinkable; these positions are misconceptions. Ship captains, system developers, and Heffalump trappers alike; *be careful.* Don't suggest your ocean liner is unsinkable, don't believe your door-lock is uncrackable, don't attempt to trap the made-up animal—refrain from assuming that it might be feasible to design a computerized device that is *perfectly* private by design. *Do*, however, embrace those driving ideals, just with a healthy skepticism towards the hubristic tendencies. In the following we describe theoretically-informed strategies to mitigate the dangers of hubris and Heffalumps.

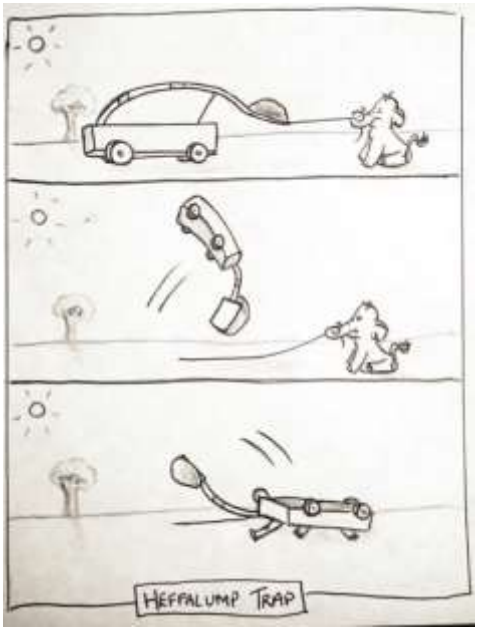

Figure 1. Depiction of a Heffalump Trap.

5 Tempering the Hubris; Designing a Philosophical Response

5.1 Object Oriented Ontology

In the following we introduce Object Oriented Ontology (OOO), a modern philosophy which can help to make sense of the complex heterogeneous contexts emerging from the IoT that are so problematic for PbD and HCD. This framework is enacted with a contemporary speculative design methodology, Design Fiction [7,19], to develop responses to the problematic aspects of PbD and HCD's Heffalump traps. We are not scholars of philosophy; hence we do not intend to discuss the nuances of OOO's place within the broader gamut of philosophy and theory. However, in order to add some context in the following we offer a short introduction to OOO, specifically within the context of computing and HCD.

Philosophically underpinning HCD's simplicity axiom in studies of Human-Comptuer Interaction, Heidegger's seminal *Being and Time* argues most objects and tools make most sense in relation to human use. Heidegger uses a hammer as an example, he says that technologies are either 'ready-to-hand' (in their normal context of use) or 'present-at-hand' (if the 'norm' is disrupted, for example if the head fell off the hammer). The metaphysics of this distinction are fascinating, but the salient issue is that the hammer comes to 'Be' through interaction with a human. As such the hammer's very existence is the product of a correlation between the human mind, and the physical world [3]. This conceptual configuration described as 'correlationism' [15]. What OOO does differently is to reject correlationism, and by doing so creates the possibility that objects have realities that are independent from human use and the mind/world correlation. Seen this way anything from a fiber optic cable, to a blade of grass, to a quantum computer, to an apple pie—may be given agency in its own ontological limelight. If we imagine that every individual concept—the fiber cable or the blade of grass—giving off a little light in this way, then we might say their collective hue is the "flat ontology" that scholars of OOO refer to [4].

"In short, all things equally exist, yet they do not exist equally […] This maxim may seem like a tautology—or just a gag. It's certainly not the sort of qualified, reasoned, hand-wrung ontological position that's customary in philosophy. But such an extreme take is required for the curious garden of things to flow. Consider it a thought experiment, as all speculation must be: what if we shed all criteria whatsoever and simply hold that everything exits, even things that don't? […] none's existence fundamentally different from another, none more primary nor more original." [3:11]

Bogost uses the famously ill-fated video game *E.T. the Extra-Terrestrial* as an example of how a single thing can be broken into many different types of OOO object. He notes that the game is simultaneously: a series of rules and mechanics; source code; source compiled into assembly; radio frequency signals; a game cartridge; memory etched on silicon; intellectual property; arguably 'the worst game ever made'; a portion of the 728,000 Atari games that were once buried in the ground in New Mexico[3]; a conglomerate of all of these. There is no fundamental thing which defines The E.T.

[3] cf. https://en.wikipedia.org/wiki/E.T._the_Extra-Terrestrial_(video_game)

video game. Instead it is all of these things simultaneously, and all of them independently of any human interaction. Contemplating what this sort of shift in ontology could mean Bogost muses "the epistemological tide ebbed, revealing the iridescent shells of realism they had so long occluded" [3].

This branch of metaphysics may seem very far removed from the development of technology, however, through a more practically-oriented approach known as *Carpentry* it can be materialized. Carpentry involves the creation of "machines" that attempt to reveal clues about the phenomenology of objects. While it's accepted that objects' experiences can never be fully understood, the machines of carpentry act as *proxies for the unknowable*. They proffer a "rendering satisfactory enough to allow the artifact's operator to gain some insights into an alien thing's perspective" [3:100]. Sometimes achieved through programming, and sometimes through other practice, "through the making of things we do philosophy" [41]—lending the theory a material tangibility is the kernel of Carpentry. The purpose of Carpentry is to give the otherwise ethereal study of ontology a very practical legitimacy:

"If a physician is someone who practices medicine, perhaps a metaphysician ought be someone who practices ontology. Just as one would likely not trust a doctor who had only read and written journal articles about medicine to explain the particular curiosities of one's body, so one ought not trust a metaphysician who had only read and written books about the nature of the universe." [3:91]

5.2 Design Fictions

All design usually seeks to change the current context, and thus to create futures by answering questions or solving problems [22]. *Speculative design* is somewhat different, it uses design to pose questions about possible futures, rather than to answer them[4]. This family of design practices does not aim to create products for market, or which solve a real problem, instead they use the traditions of design in order to elicit insights and provoke new understandings [1,8,9] (a stance that is central to 'Research through Design' [10,12]). The speculative design landscape is quite broad[5] however the specific approach we employed in this work is *Design Fiction*.

[4] "A/B" is an excellent keyword based summary of the contrast between affirmative and speculative design [30].

[5] Dunne & Raby's book [9] provides a thorough overview of speculative design practice and Tonkinwise's review of the book offers some useful critique of speculation tooå [39].

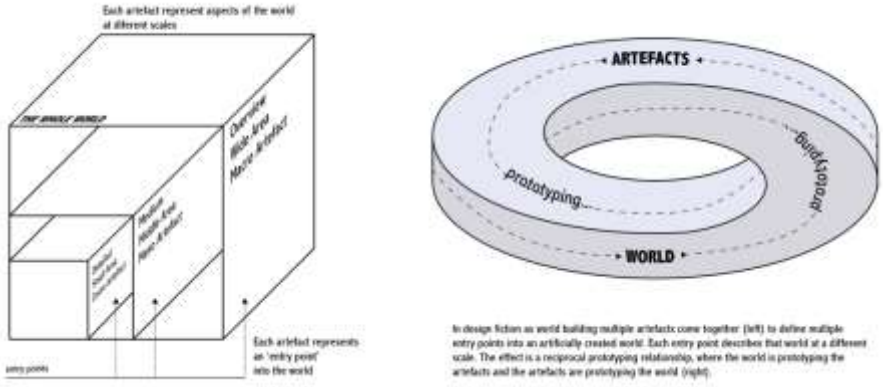

Figure 2. Design Fiction as World Building

There continues to be much disagreement about the 'best' ways to do Design Fiction, but the 'Design Fiction as World Building' approach [7] is the one we adopted with this work. Doing Design Fiction this way involves designing a series of artifacts which all contribute to the same fictional world. Individual artifacts act as 'entry points' in to the fictional world by depicting parts of it at a range of different scales (figure 2). This results in a reciprocal prototyping effect; the artifacts define the world, the world prototypes the artifacts, which, in turn, prototype the world.

We utilize Design Fiction this way in a form of Bogostian Carpentry. In Bogost's examples he explores the inner world of objects by using computer code. The flexibility of code allows him to, effectively, 'play God' within that realm. The demiurgic quality afforded Bogost by using computer code also exists when building Design Fiction worlds. However, instead of functions, APIs and code of the computer's domain, it is the essence of Design Fiction worlds—and the designed things that define them—that are the tools of this particular creationist trade.

The World's First *Truly* Smart Kettle. Employing the world building approach, we attempted to enact Bogostian carpentry in the design of a smart kettle—the kettle is branded as *Polly*, in reference to the nursery rhyme *Polly Put the Kettle On*. The contours of Polly's world are crafted through the creation of various artifacts, including a fictional press release for the kettle, packaging materials, and user interfaces. The press release describes many of the kettle's features, these include smart notifications, integration with social media, voice commands, energy tracking, location-based boiling, and the trademarked *JustRight* smart fill meter. Some of these features are prototyped in user interface designs (e.g. figure 3) and the artifacts aim to provide historical context to the Polly world too: the product was originally crowdfunded before subsequently being bought out by *Amazon's IoT* division; it is regulated by a government organization, and in order to achieve its accreditation it must utilize the *Minimum Necessary Datagram Protocol* [cf. 20,22].

Figure 3. Polly's OOO-inspired timeline and volumetric data graph.

When building Polly's fictional world we built from the assumption that continuing IoT adoption will result in even more ubiquity of data collecting devices [35]. Among these, presumably devices such as kettles will (continue to) collect data too. Today, the visibility of the data shared by these devices is at best opaque and at worst absent, isolating the user from the underlying data transactions. While PbD principles *can* protect the user from unwanted or nefarious processing of their personal data, on occasions where that sort of processing is part of the to facilitate the device's functional requirements, the best alternative would be to communicate the nature of the data transactions rather than disguising them. We may liken this to an autonomous car that would choose an optimized route to its destination. Most of the time routing designed to reduce journey times are desirable but *if* the car was designed in such a way that it would not reveal precisely what that route was, it would likely engender a feeling of distrust. Responding to this need we constructed two key features in Polly's fictional world.

Figure 3 (left) shows timeline depicting events taking place over the course of a day. From the timeline, we can tell that, in data terms, Polly was dormant for over 4 hours since the 'daily cloud pingback', which uploads usage data to the cloud and downloads configuration, security, and update data from the cloud. We can also see Polly was removed from its base, partially refilled, at which point the kettle's software anticipates it may be boiled soon. We can see that removing the kettle from the base and refilling it result in immediate sharing of data to the cloud. The anticipation event however does not share data to the cloud but does share data with the home's smart meter and other appliances to inform them of an impending power-consumption spike.

The righthand side of Figure 3 depicts the volume of the data uploaded from Polly, downloaded *to* Polly, and moving around the local network. This display differs from the timeline in that we cannot tell from it *why* data is moving around. However, what we *can* tell is the relative amount of data this smart kettle consumes and generates, as well as the relative volume of those transactions. Both displays are intended to be used in conjunction with each other such that Polly is quite transparent about to what it communicates and for what purposes. Based on the examples we can infer that Polly downloads much less data than it uploads. The specific reason for the upload/download disparity is not important, rather the takeaway point is that by utilizing Carpentry and Design Fiction, considering the reality of the kettle itself and giving the kettle's Object

Oriented perspective as much weight as the user's perspective *and* the manufacturers perspective, a more egalitarian interface can be designed that doesn't detract from the usability forwarded by HCD or the privacy credentials of PbD, but that *does* reveal the reality of what is happening and why, thus detracting from the dangers of hubris.

Orbit, a Privacy Enhancing System. This project was in part motivated to explore how the European Union's GDPR may impact on user/technology interactions. We were minded to develop a system that could obtain GDPR-compliant consent in a modern, simple and transparent way. Although legal precedents are yet to be tested and established in court, the articles of the GDPR theoretically protect various rights including: the right to be aware of what personal data is held about an individual; the right to access personal data; the right to rectify inaccurate data; the right to move personal data from one place to another; the right to refuse permission for profiling based on personal data; the right that any consent obtained relating to personal data must be verifiable, specific, unambiguous and given freely.

The process by which users consent to have their data collected and processed is an area of particular contemporary relevance. The alleged involvement of British marketing company Cambridge Analytica in Donald Trump's election victory and how, if this is shown to be true, consent was gained for the collection and processing of data from Facebook, is one factor driving interest in consent. Although some advances have been made in recent years—for example pre-checked boxes and non-consensual cookie usage were both outlawed in Europe in 2011[6]—tick boxes for users to indicate they have understood and agree to conditions of use are still the norm. There are fundamental problems with this approach, the most obvious of which being that while users often tick boxes saying they have read terms and conditions, the tick is no indication of whether they have *actually* read the text, nor whether they have understood it. In one study only 25% of participants looked at the agreement at all, and as little as 2% could demonstrate comprehension of the agreement's content [28]. User agreements that obtain a wide spectrum of consent, whereby a user gives *all* the permission a device or service could ever possibly need, stifle users' agency to be selective about which features of a system they would like to use (which in turn seems to contravene the GDPR-protected right for specific and unambiguous consent). These systems also fail to account for changes over time; once consent has been gained it is frequently impossible (or very difficult) to remove or change the nature of the consent.

Again using the Design Fiction world building approach, we decided to use an IoT lock device to build the world around. Inspired by IoT locks that already exist on the market[7] the fictional lock was imbued with the following features:

- Using short-range radio instead of a key;
- Location-based access (geofencing);
- Temporary access codes (for guests);
- Integration with voice agents (e.g. smart assistants);

[6] http://www.bbc.co.uk/news/world-europe-15260748

[7] cf. http://uk.pcmag.com/surveillance-cameras/77460/guide/the-best-smart-locks-of-2017

- Integration with other services such as If This Then That (IFTTT).

Each feature has a different relationship with collected data, where data is stored, and how it is processed. Using a short-range radio (NFC) instead of a key only relies on data inside the users own network; location-based access requires that data be accessed and stored by the lock company; utilizing services like IFTTT would lead to data being shared with any number of 3rd parties. Given that our purpose was to explore GDPR-compliant consent mechanism, our crafting of the Design Fiction only paid brief attention to the technical implementation (we assumed that the lock would utilize an IoT radio standard such as ZigBee and that suitable APIs facilitate integration with external services such as IFTTT).

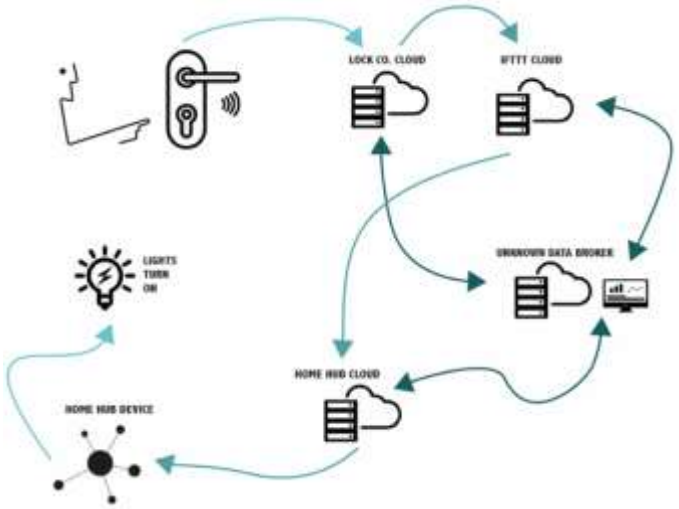

Figure 4. Diagram showing how a user opening the door may trigger a number of possible data flows around the constellation, and that there is no single end point.

Our original aim with this project was to design a map that could be used during a consent procedure to show to a user what data goes where so that they would be "informed by design" [21]. However, this aim was immediately challenged by the vast number of possible variations, even within a relatively small and straightforward IoT context. Figure 4 illustrates a scenario with an IoT lock which has been configured to turn on a smart lighting system when the user opens their door. While the cause and effect are simple and clear to the user (opening the door makes the lights turn on), there actually several cloud-based services behind the scenes that are necessary to make the hardware work. There may also be unknown 3rd parties using the data too (e.g. data brokers). Hence, to turn this into a map that details precisely where data goes, when, and in what circumstances, is simply not possible. A significant factor driving this challenge is that each specific situation needs to be treated as an ad hoc scenario, as something completely unique [31].

In order to progress some the design parameters had to be amended. Initially we made our investigation more tightly scoped, rather than addressing GDPR combability per se, we focused solely on personal identifiability. Next, it was necessary to forget the reducible concept of a map that would represent specific and quantifiable measures of probable risk and accept that any map would require much more extensive use of 'shades of grey'. As a result of these changes our experiment with OOO went in directions we had not predicted.

While our original intention was that OOO's tiny ontologies would provide us with means to investigate the lock, the associated data streams, and potential users. Our attempt at carpentry, we thought, would lead us to have a deeper understanding of those objects directly. Contrastingly, however, what came to pass is that our carpentry resulted in the creation of an entirely original object (complete with its own tiny ontology). The purpose of this new object is to provide a new lens for looking at collections of IoT devices, platforms, the data that mediates between these, and the people that use them.

These new objects—referred to as Orbits—communicate the relative likelihood that a person may be identified based upon on device use. They present this in a fashion that distinguishes between data held locally, with known providers, or with unknown 3rd parties. These 'maps' provided some means to bridge between the vast gamut of possibilities in the computer-world and the succinct concreteness of judging acceptability in the human-world. They facilitate value judgements.

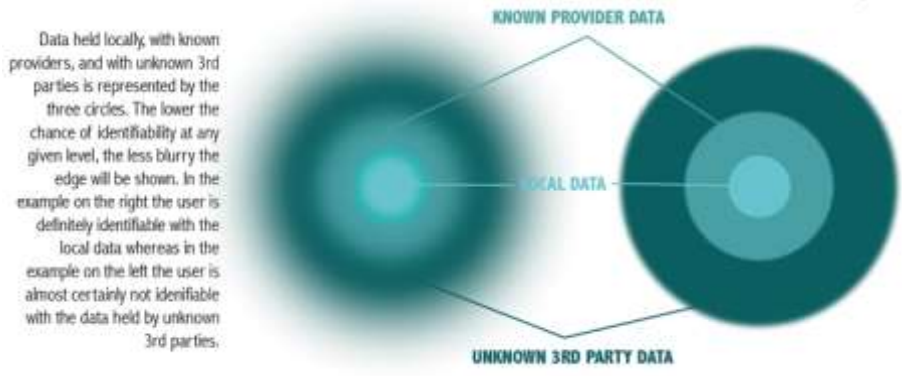

Figure 5. Example identifiability Orbits (the name 'Orbit' stems from a visual similarity to the diagrams used in the Bohr model of the hydrogen atom[8]).

The privacy Orbits map IoT systems, the data they utilize, and communicate the likelihood of identifiability based on data held in different places. The 'levels' (i.e. each concentric circle) represent data that is held locally, with known providers, or with unknown 3rd parties (see labels in Figure 5). The definition (blurriness or sharpness) at the edge of each level describe the probability, or certainty, of the user being identifiable based on the data at that specific level. If the inner-most level has a pin-sharp edge, then it is almost *definite* that the user could be identified based on those

[8] https://en.wikipedia.org/wiki/Bohr_model

data (e.g. the right-hand diagram's 1st level in Figure 5). Blurrier levels mean that the chance of identifiability is reduced (e.g. the left-hand diagram's 3rd level in Figure 5.)

The Design Fiction world we had created was a useful tool to then import the identifiability Orbits into, and to prototype how they might be used. We created a short film that shows a user installing a new IoT smart lock device in their home[9] using a voice interface and a supporting app. In essence the user is provided with a slider which enables or disables all the possible functions of the lock, the Orbits communicate how the associated changes in data flows impact on identifiability.

The same scenario may be extended to show the implications of dynamically modifying settings, for example to temporarily provide access to a delivery agent using a system similar to Amazon Key[10]. If the user has configured their system for maximum privacy (or, minimal identifiability) then Orbits could be used to temporarily provide access to the 3rd party and to show the user what the impact on data flows would be. Though this interaction is clearly achievable, it raises a host of other questions relating to the temporality of consent. For example, if a user gives consent for their data to be used by a 3rd party for a few hours, what happens to that data after those hours have elapsed?

4 Discussion and Conclusions

Our OOO-informed Design Fictions work within boundaries of the following sentiments: "the Internet must be grasped in metaphorical terms" [29] and that "Security by design and privacy by design can be achieved only by design. We need a firmer grasp of the obvious" [32]. Of course, acting on such sentiments is easier said than done, particularly when each of the constructs that we deal with—IoT, PbD and HCD—are all *suitcase* terms with multiple possible meanings. Because of this network of problematic aspects, we assert that drawing on philosophy, and employing speculative design, is a productive way to begin to unpack the problem (as opposed to more directly applied/engineering-led approaches). The examples we have provided above are intended to be used in two ways. First, we wish to forward the method itself: enacting Bogostian Carpentry as a way of practicing OOO to address the complexities of PbD and HCD in an IoT context. This conclusion is relatively straightforward; we invite other researchers and technologists to apply a similar method and in doing so research the concepts further. Second, using Design Fiction as a method of Research through Design [10,12], we offer the following primary contributions which may be directly applied by technologists.

Augmenting HCD with Constellations. Our critique and exploration of HCD is not meant unkindly. We acknowledge and applaud the rich history that HCD has, and rather than calling out shortcomings we wish to augment it for the 21st century. Thus, we propose the 'Constellation' design metaphor. This is a wrapper for the complexities of OOO and calls upon designers, developers and analysts to understand and acknowledge

[9] https://youtu.be/A37SmnNFstA

[10] https://www.theverge.com/2017/10/25/16538834/amazon-key-in-home-delivery-unlock-door-prime-cloud-cam-smart-lock

multiple different perspectives in their products. Just as the constellations in the night sky appear different depending on where you stand, the constellations of devices, data, networks, and users of the IoT appear different depending on whom you are. Rather than obfuscating this complexity, interfaces such as those exemplified in Polly and Orbit, should communicate and reveal the complexity so as to inform all parties of any relevant others' interests, activities, and agency. In doing so, the otherwise well-developed tools in HCD's toolbox, may be utilized and leveraged, in order to produce technologies that deliver on the promise of the IoT without compromising users' interests.

Humbling the Hubris; Toward *Informed by Design.* Precisely echoing our exploration of HCD, the perspective we present on PbD is not a scornful one. However, we cannot escape that the temptation to use guidelines and principles as a kind of 'safety blanket' beneath which technologists may hide *if* they hubristically argue that 'because I have ticked the boxes my system design is good enough to protect privacy'. Systems should be designed in such a way that the potential conflation of understanding relating to privacy, security, and data protection by design (and/or) default is reduced—this may be achieved by purposeful disambiguation. This disambiguation may involve acknowledging that manufacturers *cannot* guarantee total privacy and explaining the factors which underpin that uncertainty (as demonstrated in the privacy Orbits in particular). The complexities of non-functional requirements, particularly in IoT contexts, should be approached heuristically; users, and every other actor in the given constellation, should be given the agency to understand any given situation for themselves.

Avoid Heffalump Traps. Adoption of IoT devices has unequivocal societal and economic benefits, but to capitalize on those benefits designers, engineers and policy-makers need to set aside beliefs that are founded on the conceptual possibility of 'perfect' systems. Such beliefs are incongruous with the unavoidable realities of privacy, trust, and security issues. Instead, the IoT needs to be designed with a considered approach that accepts IoT devices definitely *do* pose problems for individuals' privacy, *but* that those problems can be tempered by subtly shifting our design paradigms such that they incorporate constellations of meaning and inform all participants in a constellation of their roles within it. To reinvent the world, we must speak a new language, and that language should ensure that Heffalump traps are not part of the vernacular.

Acknowledgements

This research was supported by the RCUK Cyber Security for the Internet of Things Research Hub PETRAS under EPSRC grant EP/N02334X/1.

References

1. James Auger. 2013. Speculative design: crafting the speculation. *Digital Creativity* 24, 1: 11–35. https://doi.org/10.1080/14626268.2013.767276
2. Nigel Bevan. 2015. How You Could Benefit from Using ISO Standards. In *Extended Abstracts of the ACM CHI'15 Conference on Human Factors in Computing Systems*, 2503–2504. https://doi.org/10.1145/2559206.2567827
3. Ian Bogost. 2012. *Alien phenomenology, or, what it's like to be a thing*. U of Minnesota Press.
4. Levi R. Bryant. 2011. *Democracy of Objects*. Open Humanities Press. https://doi.org/10.3998/ohp.9750134.0001.001
5. Ann Cavoukian. 2012. Operationalizing privacy by design. *Communications of the ACM* 55, 9: 7. https://doi.org/10.1145/2330667.2330669
6. Ann Cavoukian and Jeff Jonas. 2012. *Privacy by Design in the Age of Big Data*.
7. Paul Coulton, Joseph Lindley, Miriam Sturdee, and Michael Stead. 2017. Design Fiction as World Building. In *Proceedings of the 3nd Biennial Research Through Design Conference*. https://doi.org/10.6084/m9.figshare.4746964
8. Anthony Dunne. 2006. *Hertzian Tales: Electronic Products, Aesthetic Experience, and Critical Design*. The MIT Press.
9. Anthony Dunne and Fiona Raby. 2013. *Speculative Everything*. The MIT Press, London.
10. Christopher Frayling. 1993. Research in Art and Design. *Royal College of Art Research Papers* 1, 1: 1–9.
11. Susan Gasson. 2003. Human-Centered vs. User-Centered Approaches To Information System Design. *Journal of Information Technology Theory and Application* 5, 2: 29–46.
12. William Gaver. 2012. What should we expect from research through design? *Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems - CHI '12*: 937. https://doi.org/10.1145/2207676.2208538
13. Joseph Giacomin. 2014. What is human centred design? *Design Journal* 17, 4: 606–623. https://doi.org/10.2752/175630614X14056185480186
14. Maximilian Von Grafenstein and Christina Douka. 2017. The "state of the art" of privacy- and security-by-design (measures). In *Proceedings of MyData*.
15. Peter Gratton and Paul J Ennis. 2014. *The Meillassoux Dictionary*. Edinburgh University Press.
16. Timo Jokela, Netta Iivari, Juha Matero, and Minna Karukka. 2003. The standard of user-centered design and the standard definition of usability. In *Proceedings of the Latin American conference on Human-computer interaction - CLIHC '03*, 53–60. https://doi.org/10.1145/944519.944525
17. Rob Kling and Susan Leigh Star. 1998. Human centered systems in the perspective of organizational and social informatics. *ACM SIGCAS Computers and Society* 28, 1: 22–29. https://doi.org/10.1145/277351.277356
18. Joseph; Lindley and Paul Coulton. 2017. On the Internet No Everybody Knows You ' re a Whatchamacallit (or a Thing). *Making Home: Asserting Agency in the Age of IoT Workshop*. Retrieved from http://eprints.lancs.ac.uk/84761/1/On_the_Internet_Everybody_Knows_Youre_a_Thing.pdf
19. Joseph Lindley and Paul Coulton. 2015. Back to the Future: 10 Years of Design Fiction. In *British HCI '15 Proceedings of the 2015 British HCI Conference*, 210–211. https://doi.org/10.1145/2783446.2783592
20. Joseph Lindley, Paul Coulton, and Rachel Cooper. 2017. Why the Internet of Things needs Object Orientated Ontology. *The Design Journal* 20.

https://doi.org/10.1080/14606925.2017.1352796
21. Joseph Lindley, Paul Coulton, and Rachel Cooper. 2018. Informed by Design. In *Living in the Internet of Things: PETRAS Conference*.
22. Joseph Lindley, Dhruv Sharma, and Robert Potts. 2014. Anticipatory Ethnography: Design Fiction as an Input to Design Ethnography. *Ethnographic Praxis in Industry Conference Proceedings* 2014, 1: 237–253. https://doi.org/10.1111/1559-8918.01030
23. Nico Macdonald, Robert Reimann, Martyn Perks, and Aaron Oppenheimer. 2005. Beyond Human-Centered Design? *Interactions*: 75–79. https://doi.org/10.1145/1013115.1013184
24. Donald A Norman. HCD harmful? A Clarification - jnd.org. Retrieved from http://www.jnd.org/dn.mss/hcd_harmful_a_clari.html
25. Donald A Norman. 1998. *The invisible computer: why good products can fail, the personal computer is so complex, and information appliances are the solution*. The MIT Press.
26. Donald A Norman. 2005. Human-centered design considered harmful. *interactions* 12, 4: 14. https://doi.org/10.1145/1070960.1070976
27. Donald A Norman. 2013. *The Design of Everyday Things (Revised Edition)*. Basic Books, New York.
28. Jonathan A. Obar and A. Oeldorf-Hirsch. 2016. The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services. In *The 44th Research Conference on Communication, Information and Internet Policy*. https://doi.org/10.2139/ssrn.2757465
29. James Pierce and Carl DiSalvo. 2017. Dark Clouds , Io $ #! + , and ? [Crystal Ball Emoji]: Projecting Network Anxieties with Alternative Design Metaphors. *DIS '17 Proceedings of the 2017 Conference on Designing Interactive Systems*: 1383–1393. https://doi.org/10.1145/3064663.3064795
30. Fiona Raby and Anthony Dunne. 2009. A/B. Retrieved October 27, 2014 from http://www.dunneandraby.co.uk/content/projects/476/0
31. m.c. schraefel, Richard Gomer, Alper Alan, Enrico Gerding, and Carsten Maple. 2017. The Internet of Things: Interaction Challenges to Meaningful Consent at Scale. *interactions* 24, 6: 26–33. https://doi.org/10.1145/3149025
32. Stuart S. Shapiro. 2010. Privacy by design. *Communications of the ACM* 53, 6: 27. https://doi.org/10.1145/1743546.1743559
33. Sarah Spiekermann. 2012. The challenges of privacy by design. *Communications of the ACM* 55, 7: 38. https://doi.org/10.1145/2209249.2209263
34. Marc Steen. 2011. Tensions in human-centred design. *CoDesign* 7, 1: 45–60. https://doi.org/10.1080/15710882.2011.563314
35. Bruce Sterling. 2014. *The Epic Struggle of the Internet of Things*. Strelka Press.
36. Lucy Suchman. 2007. *Human-Machine Reconfigurations: Plans and Situated Actions*. Cambridge University Press, Cambridge.
37. Paul Taylor, Steven Allpress, Madeline Carr, Jim Norton, and Liane Smith. 2018. *Internet of Things: Realising the potential of a trusted smart world*. Retrieved from https://www.raeng.org.uk/publications/reports/internet-of-things-realising-the-potential-of-a-tr
38. Vanessa Thomas, Christian Remy, and Oliver Bates. 2017. The Limits of HCD. In *Proceedings of the 2017 Workshop on Computing Within Limits - LIMITS '17*, 85–92. https://doi.org/10.1145/3080556.3080561
39. Cameron Tonkinwise. 2014. How We Intend to Future Review of Anthony Dunne. *Design Philosophy Papers* 12, 2: 169–187. https://doi.org/10.2752/144871314X14159818597676
40. Nicholas Vollmer. 2017. Article 25 EU General Data Protection Regulation (EU-GDPR). Retrieved January 15, 2018 from http://www.privacy-regulation.eu/en/article-

25-data-protection-by-design-and-by-default-GDPR.htm
41. Ron Wakkary, Doenja Oogjes, Sabrina Hauser, Henry Lin, Cheng Cao, Leo Ma, and Tijs Duel. 2017. Morse Things: A Design Inquiry into the Gap Between Things and Us. *Proceedings of the 2017 Conference on Designing Interactive Systems*: 503–514. https://doi.org/10.1145/3064663.3064734
42. Summaries of Articles contained in the GDPR. Retrieved September 15, 2017 from http://www.eugdpr.org/article-summaries.html
43. 2015. ISO 9241-210. Ergonomics of human-system interaction -- Part 210: Human-centred design for interactive systems. *Standardization, International Organization for*. Retrieved from https://www.iso.org/standard/52075.html