Adaptive Architecture: Regulating Human Building Interaction[1]

Lachlan Urquhart*, Holger Schnädelbach* & Nils Jäger+

**School of Computer Science, University of Nottingham, Nottingham, UK*

+School of Architecture, Building & Civil Engineering, Loughborough University, UK

Contact Author: Lachlan Urquhart, lachlan.urquhart@nottingham.ac.uk, School of Computer Science, Jubilee Campus, University of Nottingham, Nottingham, UK, NG8 1BB.

Biographies:

Dr Lachlan Urquhart is a Research Fellow in Information Technology Law at Horizon Digital Economy Research, University of Nottingham, UK.

Dr Holger Schnädelbach is a Senior Research Fellow in the Mixed Reality Lab, School of Computer Science, University of Nottingham, UK.

Dr Nils Jäger is a Lecturer in Digital Architecture in the School of Architecture, Building & Civil Engineering, Loughborough University, UK.

[1] Presented at BILETA 2018, 10-11 April, '18, University of Aberdeen and was awarded the Taylor & Francis Prize (on behalf of the *International Review of Law, Computers & Technology*)

Adaptive Architecture: Regulating Human Building Interaction

ABSTRACT: In this paper we explore regulatory, technical and interactional implications of Adaptive Architecture, a novel trend emerging in the built environment. We provide a comprehensive description of the emergence and history of the term, with reference to the current state of the art and policy foundations supporting it e.g. smart city initiatives and building regulations. As Adaptive Architecture is underpinned by the Internet of Things (IoT), we are interested in how regulatory and surveillance issues posed by the IoT manifest in buildings too. To support our analysis, we utilise a prominent concept from architecture, Stuart Brand's Shearing Layers model, which describes the different physical layers of a building and how they relate to temporal change. To ground our analysis, we use three cases of Adaptive Architecture, namely an IoT device (Nest Smart Cam IQ); an Adaptive Architecture research prototype, (ExoBuilding); and a commercial deployment (the Edge). In bringing together Shearing Layers, Adaptive Architecture and the challenges therein, we frame our analysis under 5 key themes. These are guided by emerging information privacy and security regulations. We explore the issues Adaptive Architecture needs to face for: A – 'Physical & information security'; B – 'Establishing responsibility'; C – 'occupant rights over flows, collection, use & control of personal data'; D- 'Visibility of Emotions and Bodies'; & E – 'Surveillance of Everyday Routine Activities'. We conclude by summarising key challenges for Adaptive Architecture, regulation and the future of human building interaction.

KEYWORDS: Adaptive Architecture; ubiquitous computing; internet of things; smart cities; built environment.

1. Introduction

"It was some years before a compromise was reached between the one hundred percent responsive structure and the rigid non-responsive houses of the past. The first psychotropic (PT) houses had so many senso-cells distributed over them, echoing every shift of mood and position of the occupants, that living in one was like inhabiting someone else's brain."

"In the cloakroom, I tried to check my anger; the senso-cells had picked up the cue and began to suck the irritation out of me, pouring it back into the air until the walls of the cloakroom darkened and seethed."

J.G. Ballard, The Thousand Dreams of Stellavista, 1962

In 1962, J.G. Ballard presciently shared his dystopian vision of adaptive buildings with the world (Ballard 2006). In his short story, *The Thousand Dreams of Stellavista*, homes are emotive entities, reverberating and contorting in response to relived memories. In one of their operational modes, the homes dramatically replay the affective state of former occupants' experiences. This can be to the horror or delight of current inhabitants, who buy the homes' based on their provenance, with celebrity homes being particularly attractive. In 2018, whilst the built environment is no longer a static entity (if it ever was), but thankfully Ballard's foretelling has not manifested, yet.

Nevertheless, we are entering the age of Adaptive Architecture where buildings will interact with and respond to occupants and their environments in dynamic ways (Jäger et al. 2017). This paper explores this shift, particularly the technical, interactional, and regulatory aspects. As the nature of architecture shifts, prototypes for new forms of human building interactions emerge, ranging from the *pragmatic* to *therapeutic* to *provocative* (H. Schnädelbach 2016). *Pragmatically*, the University of Nottingham Jubilee campus has an environmental control system where temperature sensors are coupled with an automated, adaptive façade to draw air through the building without human intervention (P. Wilson 2008). *Therapeutically*, wellbeing applications using biofeedback for building adaptivity are emerging, deploying breathing or heart rate sensors to detect the emotive state of users. Examples include Breathing Space and ExoPranayama projects, which were deployed in care homes and yoga classes respectively (Moran et al. 2016). *Provocatively*, artistic applications have emerged too, such as Beesley's aerial, living structure 'Astrocyte'. This immersive experience involves a glass sculpture, aesthetically akin to a hybrid of a star & nervous system, which reacts to viewers using light, vibrations and sound (Thorns 2018).

Adaptive Architecture will recalibrate the nature of human-building interactions, mediating how we negotiate our relationships and everyday lives in those spaces (H. Schnädelbach et al. 2017). Interactions will range from ephemeral to persistent and embodied (Jäger, Schnädelbach, and Hale 2016; Dourish 2004); from low to high tech; from personalised to generic.

Many of these applications are heavily data driven, often utilising personal data, relying on different data collection approaches, both passive (e.g. ambient sensing of CO_2 or movement) and active (e.g. users speaking to interfaces via conversational agents). Converging with technological trends such as the Internet of Things, Smart Cities/Homes, and Machine Learning, new forms of ambient intelligence are set to be embedded in the built environment. This includes mundane fixtures & fittings such as smart toilets, kitchen counters and mirrors, to smart building materials and adaptive public structures e.g., bridges (P. Verbeek 2017) and parks (Smaniotto, Chair, and Técnica 2017).

As human building interactions are redefined, regulatory challenges, particularly around privacy and security emerge. To better understand these, we draw on a concept popular in computing and architecture: Steward Brand's Shearing Layers model of Change (Brand 1995) . His model provides a means to conceptualise the different sites of change within a building. These shift from the longitudinal, static elements, such as the building site or structure, down to the more dynamic, moveable aspects of the space, like furniture or possessions. Accordingly, we are interested in exploring how this model can inform conceptual discussions around technical, regulatory and interactional aspects of new data driven Adaptive Architecture applications. To do this, our structure is as follows:

Firstly, we provide a more comprehensive description of the emergence and history of Adaptive Architecture, acknowledging the current state of the art. We consider policy foundations supporting this trend too. Secondly, look at some of the challenges emerging from the Internet of Things, a key underpinning technology for Adaptive Architecture. Thirdly, we introduce Brand's Shearing Layers model, providing our proposed Shearing Layers model for Adaptive Architecture. Fourthly, we introduce three cases of Adaptive Architecture we will be exploring in more detail (Nest IQ; ExoBuilding & the Edge). Fifthly, we frame the technical, regulatory and interactional challenges through analysis of our three examples and using the Shearing Layers model. This involves consideration of 5 key themes: Physical & Information Security; Establishing Responsibility; Occupant Rights over Flows, Collection, Use & Control of Personal Data; Visibility of Emotions and Bodies in Adaptive Architecture & Surveillance implications of Monitoring Routine Activities. We conclude by summarising key challenges for Adaptive Architecture, regulation and the future of human building interaction.

2. Adaptive Architecture?

a) The Emergence of Adaptive Architecture

Stewart Brand (Brand 1995) famously stated that all buildings can adapt. All that is required is enough time and the right set of tools. Going beyond 'standard buildings' that can be adapted over time, *Adaptive Architecture* is concerned with buildings that are specifically designed to be adaptive to their environment and to their inhabitants (Holger Schnädelbach 2010). Adaptive buildings have a long tradition, enabling inhabitants to control how certain spaces looked, felt, or functioned. For example, tents allowed nomadic cultures to change their geographical location and adapt to the seasons by altering the shape and materiality of the tents (Kronenburg 2012). Similarly, Japanese residential architecture of the Heian period (794-1185 CE) became adaptive to function and use of the space by allowing both the division of interior spaces with mobile screens and the full opening of exterior walls. This began to blur the threshold between interior and exterior (Paine 1981).

Cybernetics, ubiquitous computing, Ambient Intelligence

In the 1960s, with the rise of research into cybernetics, "the scientific study of control and communication in animals and machines" (Wiener 1948), a qualitatively new form of architectural adaptivity emerged, led by Gordon Pask. Frazer describes Pask's view of architects as "system designers" (Frazer 2001), especially of self-organising systems using artificial intelligence and feedback loops, which initially targeted interaction between the designer and the system, not the inhabitant and the system. Pask was a driving force behind sensor-augmented environments that responded both to

inhabitation and environmental changes. He consulted on Cedric Price's Fun Palace (Mathews 2006), which was designed to be an interactive space, using sensors and response terminals to allow "endless" spatial and activity options to play out. These early forms of integration of computing infrastructure and architecture soon led to an entirely new understanding of how computers penetrated daily life, becoming pervasive and ubiquitous.

Mark Weiser envisioned computers becoming so fully integrated in every aspect of life and every built environment that they would essentially disappear into or blend with the background (Weiser 1991). His seminal text also ushered in a new era of computing research called Ambient Intelligence. As stated, for example, by (Nijholt, Zwiers, and Peciva 2009), Ambient Intelligence requires the constant creation and maintenance of user profiles, which typically contain the user's "preferences, interests, characteristics, and interaction behaviour". Obtaining such personal data can be achieved through active input by the user, remote sensing, and machine learning. Lino et al. argue that, based on a dense user profile, the ultimate form of adaptation would be a proactive space that "predicts user needs and actions according to a model" (Alves Lino, Salem, and Rauterberg 2010, 356).The authors also describe reactive (user input required), interactive (dialogue between user and system), perceptive (implicit user input, such as activities, to deliver preference-based services), and receptive (context-aware delivery of custom services) systems as progressively more adaptive systems, culminating in the aforementioned proactive systems.

Internet of Things, Smart Homes, & Experimental Prototypes.

Cybernetics, pervasive/ubiquitous computing, and ambient intelligence currently find expression in the consumer market and experimental research prototypes. The former takes various forms as part of the Internet of Things.

Objects of the Internet of Things, such as *smart cups* (Bradshaw 2018), *sleep robots* (Somnox 2018), or always-on *smart speakers* (Van Camp 2018) are part of ecologies of devices, appliances, and other equipment in the home that are meant to make life more convenient, efficient, or safer. Many of these devices collect personal data and store or compute this data in the cloud, such as drink temperature preferences (smart cup), sleep habits and patterns (sleep robot), or voice patterns and personal preferences (smart speakers). In combination, these typically become part of so-called 'smart homes'. They are becoming increasingly common and can be described as residential buildings with built-in sensors and actuators. These include presence sensors coupled with smart thermostats and/or burglar alarms, programmable lights and heating systems, and access control via security cameras, key fobs. Integration with machine learning is also possible, for example, *security cameras* (see below) equipped with facial recognition software, which distinguish home owners from potential burglars, with entry door access systems.

Experimental prototypes of Adaptive Architecture, on the other hand, explore technology, interactivity (via various personal data streams), materials, and computation in different ways. These explorations often use personal data, which they obtain both actively, via sensors worn by inhabitants and passively, through sensors embedded in the environment. Depending on the approach to interactivity, prototypes have been classified as digitally driven (Bier and Knight 2010), responsive (Bullivant 2006), interactive (Fox and Kemp 2009), dynamic (Kolarevic and Parlac, n.d.), and robotic (Green 2016). We now consider a few prototypes showcasing the state of the art in Adaptive Architecture.

Many Adaptive Architecture environments implement a relatively simple, reactive interaction loop, similar to the feedback systems described by Pask and falling

into Lino et al's categories of reactive, interactive and perceptive systems. For example, the motion of inhabitants can be coupled with the motion in a prototype like Glynn's *Reciprocal Space* (Glynn 2005) or *ExoBuilding* (Schnädelbach, H., Glover, K., & Irune 2010; Schnädelbach, H., Irune, A., Kirk, D., Glover, K. and Brundell 2012). ExoBuilding, which we discuss in detail later, senses the respiratory movements of the abdomen alongside heart rate and galvanic skin response, which enable it to respond to an inhabitant's physiological behaviour via environmental actuations, such as movement (breathing), sound (heartbeat), and graphic projections (skin response). The *Open Columns* prototype senses a derivative of physiological data, namely CO_2 as a product of exhalation, to disperse people when indoor CO_2 levels reach pre-defined levels (Khan 2010). Similarly, (Jäger et al. 2017), using real-time physiological data, designed a system to directly influence an inhabitant's breathing frequency without their knowledge and control.

The most complex examples draw on machine learning approaches, mining recorded behavioural data over time to enable better profiling and decision-making of the adaptive space/building. Taking adaptivity to Lino et. al's highest level of adaptivity, a proactive space, researchers have also explored the use of user-centric data to instil environments with computational agency (Alves Lino, Salem, and Rauterberg 2010). Such environments can both follow and respond to inhabitant behaviour as well as instigate behaviours of their own in response to occupant presence and activities. One of the very few functional and evaluated prototypes in this category is *Ada*, which provides multiple inhabitants with a playful and engaging experience, developed for the Swiss Expo 2002 (Eng et al. 2003). Sensing its occupants using vision, sound, and touch detection enables Ada to facilitate interactions between multiple inhabitants and multiple parts of the same interior space.

Similarly, Mozer's *Adaptive House* (Mozer 2005) and *pervasive healthcare* propose continuous, context-aware, embedded health monitoring of people wherever they are (Varshney 2007). Further, smart lifts combine data from card readers and destination selections to create more efficient circulation and to provide occupancy information (Busta 2017), proposed concepts to bring personalised architectural responses to hotel occupants (Hecht, Mayier, and Perakslis 2014), while urban lighting senses the presence of people to create light patterns depending on occupancy levels and movement (Poulsen, Andersen, and Jensen, 2012). Schnädelbach maintains examples of emerging Adaptive Architecture within his Framework (H. Schnädelbach 2016).

Having considered the history and technical state of the art in Adaptive Architecture, we now want to consider policy shifts which are ushering in this trend.

b) Policy Foundations

Embedding IT infrastructure into the built environment underpins the Adaptive Architecture trend. Within the UK, legislative and policy efforts seek to integrate networking and sensing into buildings, creating the foundations needed. Globally, government and industry led smart city investment initiatives and demonstrators represent the high profile financial and political drive to smarten the built environment (Kitchin 2014). Many of these require retrofitting IT to existing building infrastructure but shifts in construction practice integrating IT into new buildings are occurring too, guided by building regulations. We explore these briefly below.

Smart Cities Initiatives. Smart city initiatives are popular globally, with industry or government led projects in Rio de Janeiro, Brazil (Gaffney and Robertson 2016), Songdo, S. Korea (Selinger and Kim 2015), Porto, Portugal (Guerra et al. 2017) or Barcelona, Spain (Tieman 2017) to name a few. The motivation for systematically

embedding IT into the fabric of the urban built environment at scale, is broadly efficiency, convenience and security. As Kitchin argues "*the smart city promises to solve a fundamental conundrum of cities – how to reduce costs and create economic growth and resilience at the same time as producing sustainability and improving services, participation and quality of life"* through the promise of IT and data (Kitchin 2015). Glasgow's government-led Future Cities project, like many across the world, sought to bring together streams of data from around the city, using 'smart city dashboards' where local innovators could access data and create new apps & services (Glasgow City Council 2013). 'Smart city in a box' solutions offered by companies such as IBM similarly offer to upgrade dated civic infrastructure to increase intelligence of how it is utilised and managed (IBM 2011). By embedding sensors, networking and actuators in the built environment applications can emerge such as intelligently rerouting rush hour traffic to minimise congestion (Mangiaracina et al. 2017) or installing more efficient, adaptive street lighting for budgetary and environmental sustainability reasons (Griffiths 2017).

Like with smart homes, human and local community interests are often neglected within smart city initiatives, with developments not engaging with impacts on civic life across the city (Thomas et al. 2016; Coletta and Kitchin 2017; Murakami Wood 2015; Nagenborg et al. 2010). As Wilson et al showed when reviewing smart home developments, a concerted focus on inhabitant needs is still missing (C. Wilson 2015), repeating Leppënen and Jokinen's much earlier critique that this is not a forefront concern in designing user experiences (Leppënen and Jokinen 2003). Addington laments the technology push that is still prevalent and calls for the design of meaningful interactions in architecture (Addington 2015) as does Aarts in the context of the Ambient Intelligence community (Aarts and Grotenhuis 2011).

When scaled up to cities, the problem remains, as Kitchin again argues, "*the realities of implementation are messier and more complex than the marketing hype of corporations or city managers portrays and there are a number of social, political, ethical and legal concerns with respect to the kind of society smart city initiatives seek to create*" (Kitchin 2015). Constructing ethically and legally compliant smart built environment needs to respect citizen rights too, requiring more user centric regulatory approaches (Urquhart 2017). As Edwards argues smart cities pose many risks to rights, as they create the 'perfect storm' of privacy and security threats including designing adequate consent mechanisms for IoT, lack of algorithmic transparency for big data, and third country data transfer with the cloud (Edwards 2016). We return to such considerations later, but for now we turn to policy in the UK driving increased IT in buildings.

BIM. In the UK, the *Digital Built Britain* agenda was launched in 2017 with the goal of creating a 'digital economy for infrastructure, buildings and services' (Innovate UK 2016). It seeks to digitise the life cycle of buildings to incorporate a better understanding of building construction and use. This also integrates with the government's *Industrial Strategy 2017* which includes commitment to upgrade UK infrastructure with increased networking. The underlying logic of Digital Built Britain is digital technologies integrated in the design and construction process can improve the effectiveness and efficiency of buildings, so they can ultimately provide better user experiences, including lower construction costs, lower energy bills, and increased wellbeing.

A key element of this is better use of building information modelling (BIM), which is concerned with creating and using digital representations of buildings and their operations. Such representations are created during design and constructions and then handed over to building owners and operators. On a practical level, BIM Level 1 involves

a hybrid of 2D and 3D computer aided design (CAD) drawings whereas Level 2 BIM, a standard demanded by government funded construction projects to date, requires collaboration via a common data environment with 'intelligent, data rich objects in a managed 3D BIM environment'('BIM Level 2' 2018). BIM requirements are making buildings more data rich. To what extent the data is used in managing the life cycle of buildings varies, as does the quality of modelling (Arayici, Egbu, and Coates 2012). Adequately integrating BIM with operational building management systems and use, beyond merely being a planning and construction tool, is a key goal of Digital Built Britain, reflecting its higher level focus on 'people, information, processes, technology' as opposed to just buildings per se (Innovate UK & Infrastructure / Project Authority 2017). Enabling secondary uses of data for Adaptive Architecture e.g. models to assist managing how occupants move through space, may become one future use for BIM.

UK Building Regulations. Alongside, higher-level aspirations to the digital built economy, more mundane building regulations are getting the UK built environment Adaptive Architecture ready. Standards have established detailed technical guidance on how to install digital communications infrastructures in homes for networking, such as the 2010 *PAS 2016 Next Generation Access* (Department for Business Innovation & Skills, Knowledge Transfer Network 2010). However, there is also legislative footing for networking provision as a utility alongside traditional water piping, gas and electricity supply. Article 8 of EU Directive 2014/61/EU, requires Member States to ensure that newly constructed buildings are equipped with a "high-speed-ready in-building physical infrastructure" to facilitate the cost-effective installation of cabling providing a minimum broadband speed of 30mbps. In England the *England Building Regulations 2010*, translate this requirement into domestic law requiring a network termination point in each building and also a common access point for distribution in buildings with multiple homes. This applies to new builds or extensive renovations and satellite and wireless communications can also be used if they can supply the correct speeds. Technical guidance to support compliance in England has emerged (HM Government 2016) and Scottish Building Standards have the same standards, for both domestic and non-domestic properties (Scottish Government 2015).

With a closer eye to Adaptive Architecture, the 2016 *NHBC Connected Home Guide*[i] explores options for embedding technology into the home, noting the importance of network speed as an enabler for smart homes (NHBC Foundation 2016), a challenge for rural homes in particular (Ofcom 2017). However, even once there is infrastructure in place, the process of adding IoT devices to make the building adaptive is a less formalised process. Despite the emergence of smart home installation engineers (IET 2017), we need to recall Tolmie et al's work on the 'digital plumbing'. This is "the actual work of installing digital technologies in a setting" which needs to be tailored to the context of the home, particularly user interactions with existing technologies and social routines (Tolmie et al. 2010). Digital plumbing represents the change and arrival of technologies in the home, and this process plays a part in those technologies being domesticated and becoming a mundane feature of everyday life. As they note, 'digital housekeeping' around home routers and networks has become commonplace in homes, with technical discussions about connectivity or failure of networks becoming everyday (Tolmie et al. 2010).

This brings concerns about actual interactions between users, IT and buildings in Adaptive Architecture to the fore. In particular, interactions between IoT devices in a home and more structural, fixed dimensions of the building itself can shape the nature of services offered, where a hybrid character may emerge. Future Adaptive Architecture

needs to reflect on how best to deal with these different layers of interaction with users, but we need to consider where the field is going first.

3. Regulation, Surveillance & Adaptive Architecture Interactions

Regulation. In this section we consider the regulatory and surveillance implications of the use of IoT in Adaptive Architecture. As Adaptive Architecture tends to utilise Internet of Things technologies, this relies upon embedded, personal data-driven sensors and actuators. From a regulatory perspective, numerous privacy, surveillance and security concerns are raised about the internet of things, and predecessor technologies such as Ubicomp (Čas 2011; Langheinrich 2001; Spiekermann and Pallas 2006; Bellotti and Sellen 1993) or Ambient Intelligence (Alahuhta et al. 2006).

Agency and oversight for IoT services is often shared and distributed between occupants and devices. Opaque device interfaces may be managed by mobile apps (e.g. Nest App), personal home assistants (e.g. Amazon Alexa, Google Home), and ecosystem management platforms (e.g. Works with Nest). This links to Spiekermann and Pallas (2006) earlier fears about UbiComp, which now tie into IoT, that such systems enables paternalism. They do this by enforcing non-negotiable binary rules that enable automatic compliance with rules, limit control over decisions and reduce user autonomy.

Other regulatory risks arise IoT enabling adaptivity for convenience whereby routine practices and behaviours are automated e.g. switching on the lights or central heating; opening and closing windows. To operate effectively, ambient technology design needs to be informed by the domestic social order and practices of the home (Tolmie et al. 2002; Crabtree and Rodden 2004). Nevertheless, the promise of IoT is that, in exchange for data, devices sense and actuate within their local surroundings e.g. the bedroom, kitchen, garden etc. Passively and actively, home occupants' personal information is offered or captured, with inputs ranging from spoken voice commands, biometric sensors & movement monitoring to room temperature and video feeds. The EU A29 WP Opinion on IoT highlight privacy concerns regarding data collected being repurposed, users' insufficient knowledge of data processing by physical objects, and inadequate consent or lack of control over data sharing between such objects (Rose, Eldridge, and Chapin 2015; Article 29 Data Protection Working Party WP 223 2014). Linked to this, Weber is concerned about the sheer volume of data being collected by devices (Weber 2015) and for Brown (2015), IoT deployed in typically private settings, like homes, gives cause for concern.

Aligning with other trends like big data analytics, cloud computing and machine learning, personal data collected by sensors is normally relayed outside of the building, to be analysed elsewhere (UK Information Commissioner Office 2017). Here personal data may be aggregated with other users' data and analysed by supervised or unsupervised machine learning algorithms to cluster information and make predictions based on perceived patterns. This translates into assumptions about the social context of use, in order to provide ostensibly appropriate feedback and action. Examples include smart thermostats ambiently monitoring home occupant movements to develop heating schedules (Yang and Newman 2013) or intelligent home security logging unexpected human presence in a room and alerting users. Accordingly, profiling is a key concern because detailed inferences about everyday life can be derived from data flows of devices and "*analysis of usage patterns in such a context is likely to reveal the inhabitants' lifestyle details, habits or choices or simply their presence at home*" (Article 29 Data Protection Working Party WP 223 2014, 6–8) Even if devices use non-personal data, they can still create more sensitive personal data through combining data streams, changing

the legalities of processing, for example, "*data on food purchases (fridge to supermarket system) of an individual combined with the times of day they leave the house (house sensors to alarm system) might reveal their religion*" (Deakin 2015, 15). With smart home ecosystems bringing together devices from different operators, this is only going to get worse. This gives pause for concern from a security perspective, as IoT creates networks devices traditionally offline, thus creating new, unanticipated vulnerabilities. These can be harder to secure and patch than web-based technologies, with physical safety and other IoT systems in the home at risk too (Brown 2015).

Other regulatory concerns around IoT include interoperability issues between devices and across platforms (Deakin 2015, 7); and establishing responsibility and liability for harm from IoT devices (Rose, Eldridge, and Chapin 2015, 38). With the former, this might impact users exercising rights, such as to data portability (Urquhart, Sailaja, and McAuley 2017).

Surveillance. Numerous authors have explored the impacts of digital surveillance in the built environment (Murakami Wood 2015; Webster and Leleux 2018; Nagenborg et al. 2010), particularly for public spaces questioning the efficacy of early CCTV in different urban spaces such as car parks (Norris and McCahill 2006) to concerns about smart CCTV using facial and gait recognition to survey train stations or subways (Neyland and Möllers 2017). In private spaces, the impact of surveillance in the home on family dynamics has been considered for smart homes (Crabtree, Tolmie, and Knight 2017; Mäkinen 2016) and as Kitchin and Dodge state, by augmenting every day, mundane, domestic tasks, it puts them under increased control with impacts for privacy and freedom (Kitchin and Dodge 2011).

At a more abstract level, surveillance embedded architecture forms new assemblages of power (Klauser, Paasche, and Söderström 2014) where 'data doubles' are tracked within 'surveillant assemblages' (D. Haggerty, Richard V. Ericson 2000) in the built environment and mechanisms of exerting social control become distributed and latent (Deleuze 1992). Resisting tracking, categorisation and social sorting of digital and physical bodies becomes difficult in practice (Lyon 2003). Some scholars argue we are witnessing a militarisation of urban space, where targeting of individuals is enabled by new information technologies for security management: "*... this latest doctrine stresses that means must be found of automatically identifying and targeting threatening people and circulations in advance of their materialization ...*" (Graham 2009, 385). In response to these wider concerns Jones et al. proposed an people-centred, ethical framework for the further development of intelligent environments (Jones, Hara, and Augusto 2015). Similarly concerned as the built environment get even smarter, through integration of affective/emotion detection technologies, responding to citizen values like privacy are key to guarding against surveillance capabilities becoming unwieldy (Andrew McStay 2017)

Adaptive Architecture Interactions. As Adaptive Architecture requires humans to interact with buildings and technology, the systems and experiences they create contain embedded values and norms that mediate users' interactions with the world around them (Latour 1992; P.-P. Verbeek 2006; Winner 1986). Accordingly, ensuring that Adaptive Architecture develops in an ethically and legally responsible manner, requires greater reflection on the values embedded within system design. With digital ethics, frameworks like value sensitive design (Friedman, Kahn, and Borning 2008), reflective design (Sengers et al. 2005), responsible research & innovation (Stahl, Eden, and Jirotka 2013), ethical impact assessments (SATORI Project 2017), human data interaction (Crabtree and Mortier 2015) can all support this.

With law, regulating Adaptive Architecture requires us to return to (Lawrence Lessig 1999) and (Reidenberg 1998) original observations of the regulatory importance of system architecture, or 'code', as a tool for social control and shaping behaviour alongside more traditional modalities of markets, law and social norms. For Lessig, 'code' is the manmade system of hardware and software, which has no inherent or immutable values/features and thus can be redesigned to different ends, as "*technology is plastic. It can be remade to do things differently*" (L Lessig 2006, 32).

With the emergence of embedded IT systems in the built environment, the interplay between traditional architectural principles & code needs to be navigated. Within geography, Kitchin and Dodge have argued software code increasingly structures space and the built environment (Kitchin and Dodge 2011). In a departure from Lessig's framing, with the built environment, there are inherent features and materials which cannot be remade in the same way software can, i.e. land ownership, structural quality of bricks, requirements for foundations, limits of physics in design etc. Whilst Adaptive Architecture does enable adaptivity, it is not limitless, and by exploring Brand's model, we get a better sense of the temporal and spatial dimensions of what Adaptive Architecture can do, and hence where to focus regulatory concerns.

4. A 'Shearing Layers' Approach to Adaptive Architecture

a) Stewart Brand's Shearing Layers Model

As we have seen above, today's Adaptive Architecture is built around notions of digital technology that have become embedded into the built environment. Technical systems of sensors, actuators and software offer new building functionality and services. Such systems are instrumental in the production and consumption of personal data to enable these services. How can such services depending on personal data be contextualised in the built environment? To address this, we draw on the well-established concept of shearing layers developed in Architecture. This model has also been utilised in the context of software development & design (Simmonds and Ing 2000). Building on work by (Duffy 1990), Brand documented buildings consisting of layers, which change at different rates (Brand 1995) . With regards to their rates of change, they are seen as relatively independent from each other, with little friction between them. Figure 1 below illustrates this.

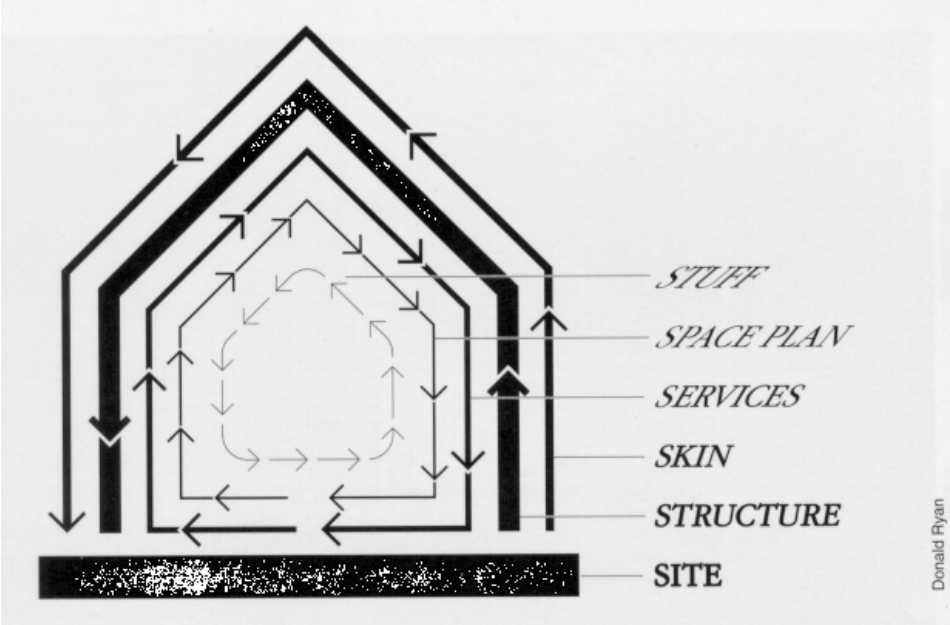

Fig 1. Brand's Shearing Layers

Site is the most rigid layer, seen as eternal, and is defined by the boundaries of the plot. The structure of a building lasts for between 60-300 years, anchoring the building to the site and it acts as the framework that all other layers are supported by. Skin covers structure on the outside and changes more rapidly with changing standards and also fashion, about every 20-30 years. Structure contains services and space plan. Services are concerned with everything from plumbing to networking and will today include the sensors and actuators of ubiquitous computing infrastructure that makes buildings adaptive (e.g. interactive, reactive, or smart) (Holger Schnädelbach 2010). Services become outdated more quickly than skins at a rate of between 7-15 years. Faster again are changes to space plan (effectively changes on and between the *level of rooms*), which in a busy office environment might change every 3 years or so, while in a home, the space plan might not change for 30 years. Importantly, the latter highlights how rates of change are not only different between the different layers, but that they also vary with the context of the building. The final shearing layer, stuff, is arguably not specifically part of the building at all. It is what people bring to the building when occupying it. The furniture, appliances, picture frames and handheld things, and this today includes numerous mobile technologies and IoT devices. Stuff can change on a minute-by-minute basis but might also last for months and years. Stuff is contained by rooms, which are part of the space plan.

In their application to the future ubiquitous research agenda, (Rodden and Benford 2003) then emphasised the different roles of stakeholders for each of the shearing layers. Inhabitants of buildings are in control of stuff and maybe space plan, re-arranging office furniture or removing and adding non-load-bearing partitions. Skin and structure are much more clearly the domain of professionals in the construction industry, at least in most circumstances. Services are an interesting hybrid in terms of stakeholder involvement. Of most interest here are those services that technically produce and consume personal data. These are now co-owned and co-managed by professionals who operate buildings (Internet providers, facility managers, building operators) and inhabitants who bring their own mobile and IoT devices, creating meshes of services

consisting in themselves of different layers. With Adaptive Architecture growing around us, digital services, regardless of who controls them, have become an increasingly important aspect of our built environment. Kitchin and Dodge have described how such digital services now pervade the architectural programme (Kitchin and Dodge 2011). People's uses of buildings can be entirely shaped by the software that runs 'on' them, with the airport terminal experience given as a prime example. This is technically achieved by integrating the personal-data relevant functionalities of the stuff, space plan and skins layers. For example, the measured occupancy levels of a building would control the required adaptive shading (both to support cooling and to avoid glare), or data from many individual mobile devices is aggregated to predict the space plan of a conference room for an upcoming meeting.

b) A Shearing Layers Model for Adaptive Architecture?

With Adaptive Architecture becoming common-place, personal data is clearly playing an important role in the built environment. Increasingly, as a by-product of the overlap of building programme and code as outlined by (Kitchin and Dodge 2011), personal data is ubiquitously produced and consumed in the built environment. Common examples include number plate recognition linked to car park access, biometric passports creating paths through customs and bank cards allowing access to travel systems. We are not focusing on the (digital) services layer (neither with regards to its hardware nor the software that drives it) in the context of this paper.

Similar to shearing layers in the built environment, categories of personal data have different life times, as has been highlighted in related work (Schnadelbach, Jager, and Urquhart 2018). Personal data might be produced and consumed to enable interactivity in the here and now, without any attempts to archive such data. For example, it has been described how personal data can create a closed feedback loop between the behaviours of people and the behaviours of adaptive environments (H. Schnädelbach 2016). In this case, personal data impacted on the rate of change within a single layer, either space-plan or stuff depending on interpretation. In contrast, archiving might be a key reason to collect personal data, as in, for example, a government census that ties personal identity to architectural site.

In this way, one might consider personal data as consisting of its own layers that are differentiated by their lifetimes, with these layers associated with specific building shearing layers. It is then a societal decision process that determines which aspects/layers of personal data are archived and which are not, which effectively moves data between layers of longevity. For example, an organisation might decide to start recording personal data that was originally only captured to enable responsive interactivity in a building (where such recording is not necessary to enable the functionality). The purpose of such a recording might be to create profiles so that an individual can expect the same functionality in an equivalent room in another part of the same building.

It is less clear that stakeholder responsibilities, from (Rodden and Benford 2003), map very cleanly to the lifetime of data, per se. In our mind, the following sets of stakeholders have an interest in the ways that personal data associates with built environments: individual inhabitants, occupying organisations (e.g. families, company departments, companies), building and data operators, building owners (which can overlap with inhabitants and occupying organisations), and regulatory stakeholders as in governments setting out planning and data regulations and their compliance agents (e.g. data and building regulation inspectors). As personal data pertains to identifiable individuals, individuals are the ultimate source of personal data, regardless of how such

data is being captured in a building. They can also immediately benefit from its use. For example, with their face recognised in a building (providing personal data), an individual might have access to a specific part of a building (drawing on a technical service that makes use of that personal data).

Occupying organisations, building and data operators and building owners are first and foremost concerned with the processing, analysis and recording of building-associated personal data. For example, an organisation will collate the movement data of their employees to optimise the use of the lifts in a building over time. For these purposes, data will often be aggregated in anonymous form. Processing is often supported by stakeholders with no direct link to that particular building, as in cloud providers that support data processing. In this respect, they are similar to oversight agencies and agents who legislate and enforce the permitted uses of personal data. Further processing by the above stakeholders can lead to the generation of new personal data, and therefore be a source of personal data. Specific examples include those where the processing of multiple anonymous data sets has led to the identification of individuals (Narayanan and Shmatikov 2008).

More importantly for the context of this paper, and as hinted at above, stakeholders are responsible for moving data between personal data layers of longevity. Each of the stakeholders has interests that impact on the lifetime of personal data. An individual might want personal data to be deleted for privacy reasons, while an occupying organisation or government archive would like to maintain records of personal data for future analysis and research. This further details the process first outlined in (Lehikoinen and Koistinen 2014), where personal data, generated and consumed on a local level becomes part of a much wider system that passes personal data from rooms, via building into the networks of the smart city, traversing and making connections between people, rooms, buildings and the urban environment. With regards to their projected life-time, personal data layers might then be seen as associated with building shearing layers (e.g. a data archive designed to last for 100 years and therefore for as long as the structure of the building the data is emanating from).

Finally, personal data is very much unlike just another shearing layer in the following sense. All of Brand's layers are ultimately tied to site. With personal data not being physical, this is not the case. Personal data is tied to recording devices (i.e. without a physical container, personal data has no existence, that container being analogue or digital). However, personal data can be copied and moved between recording devices. In addition, recording devices (e.g. from USB cards to server hard drives) can be moved themselves, while it is relatively unlikely that server rooms that are installed as part of a building's service layer are moved with its data, in practice). We have already discussed how stakeholders cause copies and moves of personal data between building and data layers associated with a single building and site. In addition, personal data can then also make connections between multiple sites in the same urban environment and beyond.

5. Three Cases of Adaptive Architecture

In the above reflection on Brand's shearing layers in the context of building-associated personal data, we have already used hypothetical examples, but Adaptive Architecture is not just hypothetical. We draw on three examples of different scales and relate those to our outline of the layers of Adaptive Architecture. The examples are 1) the Nest Cam IQ home surveillance camera, which can be clearly associated with Brand's stuff layer, 2) the ExoBuilding biofeedback environment, which fits into the space plan layer and 3) The

Edge, environmentally friendly and adaptive office building, which covers all layers from site to stuff.

Nest Cam IQ (Pardes 2017) is a home surveillance camera that offers face recognition, automatic zoom and tracking of faces, motion- and sound-triggered alerts, and interoperability with other smart devices. Once installed and networked, it allows inhabitants to view and record video and audio data remotely for surveillance purposes. The product can be trained to recognise known people and it will send automatic alerts when someone unknown is seen by the camera. Via two-way audio and video, homes can be checked on remotely and this can also be used as a social communication medium. It is typically installed by an individual or a family.

Nest Cam IQ very much falls into Brand's stuff layer of artefacts in the home that can move and change on a relatively quick time scale. Its technical properties demonstrate how such digital stuff becomes integrated into the services layer of the home, creating a mesh of IoT devices and building services, as it uses broadband and it integrates with other devices (e.g. thermostats, burglar alarm). The lifetime and uses of the produced personal data are managed by inhabitants via a service plan of the supplying company, allowing the storage and retrieval of data. This plan relies on a cloud service, highlighting how personal data transcends the stuff, services and site layers, becoming physically disassociated with the building.

ExoBuilding is a room that follows the breathing, heartbeat and electro-dermal skin response (e.g. indicating levels of relaxation) of a single person in its movement, soundscape and imagery (Schnädelbach, H., Glover, K., & Irune 2010). When a person breathes in, the room increases in size and when they breathe out, the room decreases in size. A person's heartbeat is sonified through a set of speakers and levels of EDA trigger the projection of a set of graphics on its fabric shell. This room was designed to experiment with making connections between personal data and adaptivity in the environment, and it was shown how this link can have a calming effect (Schnädelbach, H., Irune, A., Kirk, D., Glover, K. and Brundell 2012). ExoBuilding captures and 'displays' personal data in the environment, feeding back on its inhabitant but also making this data public to anyone who is present in the same room. Data is stored locally for further analysis and there is no need for the room to be networked. Data capture is via a personal IoT device (a physiological data logger, which could be a fitness tracker or smart watch in future) and this device is linked with the services layer of the ExoBuilding.

For the context here, ExoBuilding is a useful example of an adaptive room, falling into the space plan layer. Via sensitive personal data (e.g. physiological data of various types), adaptivity is such that the room changes second by second, accelerating layers of change in the space plan layer, beyond what Brand envisages. It also demonstrates how personal IoT devices can become integrated into services layers without requiring access to the cloud. Personal data remains in the room, while it is 'published' there, as the behaviour of its inhabitant is visible to everyone nearby. If used in a home, the lifetime of the personal data produced would be managed by its inhabitants, who might decide that their record of physiological data might be useful for fitness training or medical support.

Finally, we briefly introduce The Edge, as an example of an integrated adaptive office building, bringing together personal IoT devices, building services, space plan use and the building skin, all impacted by personal data (Randall 2015).The building offers around 1250 hot desks to around 2500 office workers. To manage building and desk usage and the building's energy consumption, it draws on data provided via a mobile app used by workers. The app tracks things like a person's schedule, their arrival time at the building and their preferences (e.g. for light levels). It enables the use of shared digital

screens and orders from the lunch menu. The building tracks number plates entering the car park, it tracks motion, light levels, temperature and humidity levels through sensors in the ceiling panels. The occupying organisation, uses this information to assign parking, rooms and desks, to change room ambiance and to provide the chosen lunch. Beyond this immediate use, data is used to optimise building use in the medium to long term (for example closing unneeded sections and to optimise energy efficiency).

The Edge demonstrates the full integration of personal IoT devices using the company's app, with the building's services layer and its skin. This integration is a fundamental part of the building design and personal data bridges between the layers. Individuals and the occupying organisation collaborate to move personal data from personal devices and cars (stuff) into usage and the ambiance of the building interior (space plan) and then to the operation of the façade (skin). The aim of this use of personal data is to deeply integrate with and affect the programme of the building, making it possible that there are only half the number of desks than there are workers, and that the building complies with the latest environmental standards. Personal data very much leaves the boundaries of devices, rooms, and the building so that it can be analysed over the long term.

This section explores a range of challenges posed by Adaptive Architecture. It involves bringing together IoT, our shearing layers model, our examples of Adaptive Architecture and regulatory concerns (primarily on data protection and security, drawing on GDPR).

Challenges of Adaptive Architecture

In this section, we use Brand's model to help us frame regulatory, interactional and technical challenges of Adaptive Architecture, framed under 5 key themes: Physical & Information Security; Establishing Responsibility; Understanding Flows, Collection, Use & Control of Personal Data; Sensitive Personal Data & Monitoring Routine Activities.

A. Managing Physical & Information Security whilst Living with Adaptive Architecture.

If we return to Ballard, we see the security implications of Adaptive Architecture going beyond informational to physical harms. The following quote from *A Thousand Dreams of Stellavista* describes the protagonist's experience of the house one evening:

"The entire house started to shake and writhe. Gripped by this seizure, the bedroom contracted and expanded like the chamber of a dying heart, the ceiling rising and falling… the walls closed in on each other. Pressing my hands against the ceiling, I felt it push downwards strongly. The edges of the floor were blending into the walls as the room converted itself into a sphere. The air pressure mounted. I tumbled over to the vents, reached them as they clamped around my fists, air whistling through my fingers…" (Ballard 2006)

Whilst not caused by a security breach, this passage hints towards the impacts of when things go wrong in the built environment, physical harm. In a security context, this could just as easily be someone hacking into the house smart locks to prevent someone exiting the house during an emergency, remotely turning down hospital heating during a cold snap or switching off office air conditioning during a heat wave.

Physical Security. Leverett et al argue that there are insufficient laws regulating safety, and changes are afoot in security engineering, because "*in the future, safety will require security as well*" (Leverett, Clayton, and Anderson 2017). Standardisation will be a complementary element to address inadequacies of cyber-physical systems.

Forming reasonable expectations for various Adaptive Architecture stakeholders' roles in protecting occupants' safety will turn to many established actors in the building industry, from building management operators and factors to landlords and occupants. However, defining parameters of responsibilities for IoT device manufacturers and service providers in addition to networking, mobile app or software vendors also need consideration. Attention from tort/delict, insurance, product liability and property law will be necessary in the future to determine where responsibility should lie for harms from adaptivity of buildings (e.g. if a landlord or occupant did not maintain adaptive windows adequately are they or the manufacturer responsible?). How decisions are reached within Adaptive Architecture applications may require greater transparency too, as establishing legal 'chains of causation' for blame or negligence if harm occurs are important for litigation. Furthermore, the degree to which agency is shared between Adaptive Architecture application and occupants could impact these judgments too (e.g. if an inhabitant knowingly did not step back when the adaptive windows were closing).

Information security, Adaptive Architecture is afflicted by the inadequacy of cybersecurity in the IoT infrastructure it depends upon. Smart toy (Hautala 2017) or baby monitor (JM Porip 2016) vulnerabilities have enabled spying on children in their own home and IP connected cameras have enabled cybercrime infrastructure, by becoming zombies in botnets (Greenberg 2017; Leyden 2017). Accordingly, ensuring applications can meet 72-hour GDPR data breach notification requirements is imperative, but incredibly hard to do in practice due to interconnectedness of IoT devices, especially across layers (Art 33-34, GDPR). However, the unpredictability of adaptivity of Adaptive Architecture adds another security dimension. If windows automatically close when room temperature reaches a certain level, there is scope for harm if appropriate kill switches are not built in (e.g. to prevent occupants being crushed if sitting in the window) or the system is compromised and used to malicious ends (e.g. ransomware that keeps all doors locked unless payment is made). General cybersecurity concerns around cyber-physical systems very much encompass Adaptive Architecture too (Urquhart and McAuley 2018).

Responsibility for Security. As our use of Brand's model showed, there are numerous stakeholders surrounding Adaptive Architecture interested in building and data management. Establishing who is responsible for security involves defining responsibilities at different layers, from planning bodies and construction industry at the site and structure layer down to vendors of IoT devices at the stuff layer. Within these, they exercise a degree of perceived agency (using supervised or unsupervised machine learning), to reach decisions beyond direct user control within Adaptive Architecture may blur responsibilities. Within the Edge building, for example, there are many interacting data driven products and services creating the worker experience such as ANPR authorising car access to parking spaces, security robots policing the property and personalised workspaces.

Responsibility is important to ensure compliance with practical legal requirements too, particularly for data controllers when dealing with information security. Under GDPR they have obligations of *integrity and confidentiality*, where data must be secured using technical and organisational measures to protect against unlawful loss, destruction, or damage (Art 5(1)(f) GDPR). Similarly, they need to ensure *data security*, by putting in place technical & organisational safeguards proportionate to data security risks are necessary, particularly use of encryption, pseudonymisation, confidentiality, integrity &

resilience testing (Art 32 GDPR). Given the temporal aspects of buildings, a point we return to below, managing security over time is another challenge, particularly as service providers no longer update or maintain their devices.

B. Establishing Who is Responsible within Adaptive Architecture.

Stakeholders. With Adaptive Architecture, like with IoT in general, establishing who is responsible for protecting occupants' personal data, information and physical security is complicated by the opacity of stakeholders around the devices and services. There is an extensive ecosystem of third parties seeking access to personal data to provide services e.g. behavioural marketers, insurance, law enforcement, social networking platforms, and this is added to by the convergence of technologies IoT involves. Big data analytics, cloud computing, and increasingly machine learning, are three enabling technology trends that bring their associated regulatory challenges and stakeholders to the table with IoT. Against this backdrop, establishing who is responsible for Adaptive Architecture security and privacy can be complex, and it is useful to consider the IoT supply chain. In 2014, the Article 29 Working Party Report on Data Protection Implications of IoT (Article 29 Data Protection Working Party WP 223 2014) mapped responsibilities onto different stakeholders (see Appendix 1), namely operating system and device manufacturers; IoT device owners and onward recipients of data; standardisation bodies & data platforms; social platforms; and application developers. To name a few, they state that all stakeholders should conduct privacy impact assessments (PIAs) prior to releasing new applications (share publicly where possible); if raw personal data is being used, delete quickly after use; create 'user friendly' methods for interacting around consent, rights to refusing processing and when providing information; provide users with more control over their data; broadly apply the principles of Privacy by Design and by Default.

Similarly, the recent *UK Government Secure by Design Report* (DCMS 2018) defined IoT security obligations onto different stakeholders, namely – device manufacturers, IoT service providers, mobile app developers and retailers. These include, *all stakeholders* providing personal data protection; *device manufacturers* ensuring no use of default passwords and software integrity; *IoT service providers* monitoring usage data for unusual activity or making services resilient to outages.

For Adaptive Architecture, various stakeholders from the built environment also need consideration. With our Nest IQ example, we still have the manufacturer, service provider, app designer etc., although, with Nest seeking to be the hub in the home through Works with Nest, these are the parent company Google. Nevertheless, how these IoT stakeholders intersect with property or building managers remains to be seen.

As we move towards human-building interaction with Adaptive Architecture, services will not be constrained to one layer, and instead may require data to move across layers. Such hybrid services will be underpinned by data moving from the stuff and space plan layers of IoT to the structure or skin, as we see with the Edge.

Stakeholders. With data protection, definitions from GDPR help us navigate the scope and breadth of the law, particularly what stakeholders are responsible. Firstly, we need to consider the law's scope. It applies to processing of *personal data*, which is defined as any information relating an identified or identifiable natural person including direct or indirect identification, using identifiers (i.e. name, ID number, location data) or factors showing their identity (i.e. physical, mental, economic, social...cultural) (Art 4(1) GDPR). Processing is similarly broad, including any operations performed on personal data including use, collection, recording, organisation, structuring, storage, adaptation or

alteration, retrieval...consultation. (Art 4(2) GDPR). The rights in GDPR belong to data subjects, who are identified or identifiable natural persons the personal data relates to. (Art 4(1) GDPR). The responsibilities for GDPR compliance largely lie with *controllers*, who are the entity that, alone or jointly, decides the purposes & means of processing i.e. IoT service provider, public authority, internet service provider. (Art 4(7) GDPR). Accordingly, navigating who is the data controller in Adaptive Architecture applications is both important and complex because of the range of stakeholders at play, as discussed below. Data controllers need to establish technical & organisational measures to ensure compliance with the GDPR, relative to likelihood & severity of risks to rights of data subjects. (Art 24 GDPR). Within GDPR, *data processors* have increased responsibilities too, as the entity processing personal data on behalf of the controller (i.e. contractually outsourced) (Art 4(8) GDPR). This may be a third-party cloud platform providing storage for a controller, or an analytics firm providing greater insights into data.

Domestic Data Controllers. An interesting question surfaces for Adaptive Architecture in the home around the limits of the GDPR Household Exemption. It states GDPR does not apply to data processing by a natural person in the course of purely personal or household activities (Art 2(2)(c) GDPR). This raises interesting questions about the extent to which domestic occupants can be data controllers within the confines of their data driven Adaptive Architecture home, and how they respond to requests to rights from visitors e.g. a family friend requesting the RTBF after visiting the Adaptive Architecture home. However, as above, how data is managed as it moves from stuff or space plan to structure or even site layers means, temporal aspects of data interactions & buildings need appreciation.EU case law has shown a narrowing of the exemption, as the recent Rynes case showed the exemption does not apply for operation of domestic CCTV pointing to public spaces, and hence the homeowner can be a controller.

C. Occupant Rights Over Flows, Collection, Use & Control of Personal Data in Adaptive Architecture

Flows & Contextual Integrity. Within buildings, the way in which space is diverse, involves different social norms, behaviours and relationships. Occupants may be families, friends or colleagues. This is contextual, and how information moves through contexts can have social implications. As Nissenbaum famously argues, privacy can be viewed as maintaining contextual integrity of information. In this model, privacy harms stem from information moving out of contextually appropriate flows enabling others to access or view it (Nissenbaum 2009) . How data moves between layers of Adaptive Architecture buildings, and between sites has clear privacy ramifications. Again, Adaptive Architecture is underpinned by IoT, and there are numerous challenges in how data flows within and between IoT devices and how services are managed. Furthermore, many IoT services rely on machine-to-machine (M2M) interactions without human oversight e.g. smart thermostats sharing motion sensing with smart alarms to detect unexpected occupancy of a room.

Collection & Specified Purposes. Some users may perceive such M2M communications going beyond what they expect, and see this as a degree of scope creep, particularly if data is accessed by third parties. Service providers need to recall that data can only be processed for defined *purposes* and cannot be used in ways inconsistent with these (Art 5(1)(b) GDPR). Machine-to-machine uses of data may be legitimised based on contractual agreement of users with terms and conditions of using such devices. There are many legal grounds for processing data of which consent is one, but others count when necessary, such as if processing in the public interest, controller's legitimate

interests, to satisfy a contract or other legal obligation (Art 5(1)(a) and 6 GDPR). In practice, these other grounds may often be relied upon as opposed to consent, due to difficulties in obtaining legally valid consent. Nevertheless, to ensure socially trustworthy human building interactions, we are particularly interested in how consent requirements within GDPR as IoT poses significant challenges to be overcome for obtaining meaningful user consent.

Consent Mechanisms. Consent must be an unambiguous agreement to data processing that is freely given, specific & informed. Statements or other oral, written or electronic affirmations are needed. (Art 4(12) and 7 GDPR). Consent must be provable, can be withdrawn at any time, & when given as part of a larger written contract, the details are flagged up in clear & plain language (Art 7 GDPR). The nature of 'ambient', latent data processing; multiple stakeholders with vested interests in accessing data (from law enforcement to marketers) and opaque flows of data create a hard environment for meaningful consent. From a user perspective, insufficient control over what devices are doing is due to lack of or partial user interfaces with IoT devices. On one hand, consent is frustrated by the heterogeneity of devices and lack of mental models' users have for interfaces (e.g. unlike with phone interfaces largely harmonised by the operating system). On the other hand, communicating information for consent purposes may use affordances of devices, for example with beeps, speech, lights and video, to overcome inadequacies of text heavy terms and conditions which users do not read due to complexity and time to read and cannot negotiate even if they did (Ewa Luger, Moran, and Rodden 2013; Urquhart and Rodden 2017).

Use, Temporality and Spatiality. When considering how this intersects with Adaptive Architecture, we have *temporal and spatial* dimensions of applications to consider. Once user consent is given it is not forever. Whilst it may be useful to preserve data within a building for provenance or cultural heritage reasons (as was the case with the Ballard story where it was owned by a famous actress) managing the lifetime of data requires attention in Adaptive Architecture. Similarly, how data moves between layers and sites means consent mechanisms need not only sit at the stuff layer (with IoT devices) but also be designed to consider how data is used at structure or space plan layers too. For end users, GDPR provides a spectrum of control rights, others considered below. But for temporality, the Right to be Forgotten is a clear right to consider. This provides users a right to data deletion without delay. If user consent is withdrawn or data is no longer necessary, controllers must comply. Generally, this right is not absolute & must be balanced against freedom of expression or public interest. (Art 17 GDPR). Adaptive Architecture applications need to consider how balances are made between the value of data being tied to a building e.g. if it's in the public interest due to being historically or culturally valuable, such as a National Trust property, or forgotten once the occupant leaves for privacy purposes e.g. in a rental situation or where they experienced traumatic break-up, divorce or death there.

Control & Portability. Short of full deletion, subjects also have a right to data portability, which means they can request certain personal data in a structured, commonly used, interoperable & machine-readable format e.g. CSV, JSON. They have a right to transmit this to another data controller. (Art 20 GDPR). This poses interesting questions around how data is moved between sites, for example when moving flats. Interestingly, the right to data portability does not exist for any statistical analysis conducted on personal data by the data controller to reach insights or to personalise services (Urquhart, Sailaja, and McAuley 2017). With Adaptive Architecture, much of the adaptivity might stem from subsequent analysis of the data to provide personalisation or value-added services e.g. from a combination of personal data shared machine-to-machine, there is a

learnt schedule for desired room lighting, temperature and size. Hence, portability of personalised adaptivity may be limited by this constraint.

Legibility, Transparency and Layers. Linked to the above point, particularly in respect of the heterogeneous interfaces is the experience of occupants in Adaptive Architecture. Human building interaction is changing, and the limited transparency of data flows is impacted by the opacity discussed above. The law is seeking to increase control over data use and legibility in how it is collected. With the former, this is done via the spectrum of control rights available, but we focus on the latter two, namely the right to data portability and to be forgotten. The rest are summarised below. With the latter, the law puts obligations on data controllers to increase transparency, access to information and accountability around how data is handled. With transparency, information provided to end users must be concise, transparent, easy to understand, and written in clear language. (Art 12 GDPR). This includes respecting the information rights of data subjects, too, as controllers should provide users information on their identity, contact details, purposes and legal grounds of collection. (Art 13, GDPR). With accountability, data should be processed in compliance with GDPR & this should be demonstrated to users & regulators through an account of actions taken (Art 5(2) GDPR). As with questions of consent with variety of interfaces, how information is communicated in Adaptive Architecture remains a challenge, particularly as it moves between layers, away from the IoT stuff layer. Furthermore, whilst we've discussed portability and the Right to be Forgotten, there is a range of other rights, to object, restrict, access, or rectify personal data (Arts 15; 16; 18; 21 GDPR)[2]. Designing mechanisms into Adaptive Architecture infrastructure that manage these various rights across layers and sites will be a challenge, as it requires appreciation of the relationship between the lifetime of infrastructure and data.

D. Visibility of Emotions and Bodies in Adaptive Architecture

A novel aspect of Adaptive Architecture is its use of affective computing (Picard 2000), as we see with the example of ExoBuilding, is the use of sensitive personal data to provide adaptivity, including biometric data. Other applications drawing on affective computing involve emotion too, for example with facial recognition and computer vision e.g. social signal processing to detect the perceived emotional state of an individual. Within GDPR, both biometrics and special categories of personal data are protected. Special Categories of Personal Data include political opinions, genetic & biometric data, health & sex life data, racial & ethnic origin, religious & philosophical beliefs, cannot be processed unless explicit consent is obtained, or processing is necessary for certain purposes. (Art 9 GDPR). Other legal grounds, like legitimate interests or fulfilling a contract, will not suffice here. Biometric data is the outcome of a technical process related to a subject's physiological, physical or behavioural attributes. It enables unique identification of the subject i.e. fingerprints. (Art 4(14) GDPR). So, with Adaptive Architecture using biometrics we need to build in safeguards to obtain explicit consent, returning us to discussions of the challenges of doing this above. More complicated is the

[2] Right to Object - Users can object to their data being processed, particularly for direct marketing. After they do so, the direct marketer must stop using it. (Art 21 GDPR); Right to Restrict - Users have a right to restrict data processing, instead of full deletion. Restricted data can only be processed in limited circumstances, namely with user consent or for the public interest. (Art 18 GDPR); Right to Access - Users have a right to know who processes their data, why, where & what data is stored, how it is used & shared. They can request a copy for a fee. (Art 15 GDPR); Right to Rectify - Users have a right to get inaccurate information corrected & incomplete data completed. (Art 16 GDPR)

parameters of when 'emotional data' becomes personal data, and this depends on being able to single out or identify an individual (Clifford 2017). Sentiment analysis on properly anonymised tweets may not qualify, but facial recognition like the example above would. However, as McStay argues, even if emotion sensing is not using personal data that *identifies* individuals, as many in the advertising sector claim, the *intimacy* of such data means protections still need to be put in place (Andrew McStay 2016). He also argues affective computing makes the body visible, and emotions machine readable, but people do not like this trend (Andy McStay 2017). Accordingly, understanding how such data moves between layers is important, particularly as if it involves inferences about emotional state of occupants e.g. in a shared tenement. Adequate protections for emotion sensing is new territory, but in any case, minimising what data is collected in the first place for functionality of the Adaptive Architecture application is a good start.

As the spaces we work or live in become more aware of our emotive states, there are discussions about how best to design feedback for individual or collective emotive states. In particular, this requires guarding against manipulation through increased awareness of our peers' state of mind (either at home or work) and similarly, any unwanted disclosures that may lead to conflict or tensions in group dynamics. Empirical research on living in smart homes already suggests the concerns of occupants having information shared within the family unit (Crabtree, Tolmie, and Knight 2017; Mäkinen 2016).

E. Adaptive Architecture, Surveillance & Monitoring Routine Activities

Lastly, like with IoT, Adaptive Architecture operates in everyday domestic or workplace settings. The daily practices of occupants can be observed, monitored over time, and stored. Accordingly, the scope for perceptions of surveillance is high, particularly given the opacity of data collection and use. IoT devices enable a detailed patchwork of inferences about everyday life to be drawn, but these may be partial or limited. Accordingly, who is observing and for what purposes shapes how such stories of domestic and workplace life are interpreted. Recent case law on covert CCTV suggests that privacy rights can be infringed unless such use is based on suspicion of malpractice or criminal activity and workers are informed of possibility of covert surveillance being used (exceptionally) incl. what it might be used for (Lopez Ribalda v Spain, 2018). How such precedent applies to covert visual surveillance systems in the Edge remains to be seen.

Increasingly, to manage the volume of data sensed by IoT devices, algorithmic decisions underpin interactions users have with devices. However, legally, unless a decision is contractual or explicitly consented to, data subjects have the right not to be subject to automated decision making with legal effects e.g. algorithmic mortgage refusal. They can request human oversight & review of decisions made. (Art 22 and 15(h) GDPR). Whether this extends to a 'right to an explanation' is a contested issue in legal scholarship (Edwards and Veale 2017; Floridi 2017; A. Selbst and Powles 2017), and how such an explanation may be created or delivered is a technical one too (Kroll et al. 2017; A. D. Selbst and Barocas 2017; Guidotti et al. 2018). Nevertheless, within Adaptive Architecture, like with other technology trends, the need for greater engagement with occupants and users about how their data is used is growing. In response to this, the legal requirement to do privacy by design and default has an increasing role to play. Technical & organisational safeguards should be built into processing by design & default to protect rights of data subjects & comply with the law. Costs, technical state of the art & degree of risk need to be reflected. (Art 25 GDPR). However, in practice, translating DP law into

more accessible forms for developers and designers remains a challenge. Efforts are being increased in the domains of privacy engineering to do this, but increasingly digital ethics has a role to play on the organisational side (Hadar et al. 2017; Colesky, Hoepman, and Hillen 2016; E. Luger et al. 2015). With AI in particular, efforts from professional computing societies, the ACM and IEEE, to create codes of practice for AI developers seek to be instructive in years to come (Association for Computing Machinery US Public Policy Council (USACM) 2017; IEEE 2016).

When thinking about how data is handled by Adaptive Architecture, the lifetime and temporality of the data is a key consideration. With the Edge for example, some interactions in the workplace will be ephemeral, and others need to be more longitudinal, e.g. designing occupant experiences to reflect the different lifespans of data may depend on tasks, more than cultural heritage requirements to preserve data in the interests of the building.

To pull together this extensive analysis, we conclude by very briefly stating the key regulatory challenges for Adaptive Architecture for each heading and reflect on the future of human building interaction.

Concluding thoughts

Physical and Information Security Management - Managing security in Adaptive Architecture is going to be a challenge due to the combination: higher risks of physical harm; poor underlying IoT device security; unpredictability of Adaptive Architecture applications; need to manage security longitudinally.

Establishing Responsibility - Establishing who is responsible for what in Adaptive Architecture is going to be complex. This is driven by the variety of new stakeholders from the built environment, coupled with the multiple building layers embedded with data driven technology. These discussions will shift depending if it is public (smart cities), workplace (the Edge), or domestic (smart home) contexts. With the latter, for example, we have a new domain for navigating the extent of the household exemption, and to what extent there will be 'smart home' domestic data controllers. As homes are bequeathed and passed through generations, will stewardship for data pass too?

Protecting Occupant Rights. Despite the variety of issues at play in this section, at its core we are interested in how to protect occupant rights over flows of data within Adaptive Architecture. With flows, collection, use and control, the trend exacerbates existing challenges for legal concepts & rights, with the additional interactional, temporal and spatial aspects of buildings to consider.

Visibility of Emotions and Bodies. The use of affective computing and biometrics within Adaptive architecture makes bodies visible in new ways, creating more intimate forms of human building interaction. The need to obtain explicit consent, reiterates that data will often be processed in buildings using other legal grounds, and this is not a good basis for the Adaptive Architecture future.

Monitoring and Surveillance. As Adaptive Architecture requires systematic monitoring of intimate, everyday practices to make inferences, the long-term surveillance of occupants could lead to real privacy harms. To mitigate this, adopting privacy by design type strategies to increase transparency of how occupants are being watched will go some way to increasing trust, and complying with legal requirements of increased algorithmic accountability.

Whilst buildings are becoming more adaptive, they change at different speeds, depending on the layers. Understanding how occupants, and their data, interact with

Adaptive Architecture is key to creating buildings they will want to live with, now and in the future. Ensuring their legal rights are protected is a key part of this. If not, Ballard's darker vision may still come to pass, nearly 60 years later.

Acknowledgements

This work was supported by the Engineering & Physical Sciences Research Council [Grant Number EP/M02315X/1] and a University of Nottingham Research Fellowship.

References

Aarts, Emile, and Frits Grotenhuis. 2011. 'Ambient Intelligence 2.0: Towards Synergetic Prosperity'. *Journal of Ambient Intelligence and Smart Environments* 3 (1). IOS Press: 3–11.

Addington, Michelle. 2015. 'Smart Architecture, Dumb Buildings'. In *Building Dynamics: Exploring Architecture of Change*, 59–68. doi:10.4324/9781315763279.

Alahuhta, Petteri, Paul De Hert, Sabine Delaitre, Michael Friedewald, Serge Gutwirth, Ralf Lindner, Ioannis Maghiros, et al. 2006. 'The Brave New World of Ambient Intelligence: A State-of-the-Art Review [Deliverable D1]'. *Safeguards in a World of Ambient Intelligence (SWAMI)*, no. January: 1–221.

Alves Lino, Jorge, Benjamin Salem, and Matthias Rauterberg. 2010. 'Responsive Environments: User Experiences for Ambient Intelligence'. *Journal of Ambient Intelligence and Smart Environments* 2 (4): 347–67. doi:10.3233/AIS-2010-0080.

Arayici, Yusuf, Charles Egbu, and Paul Coates. 2012. 'Building Information Modelling (BIM) Implementation and Remote Construction Projects: Issues, Challenges, and Critiques.' *Journal of IT in Construction* 17.

Article 29 Data Protection Working Party WP 223. 2014. 'Opinion 8 / 2014 on Recent Developments on the Internet of Things'. JOUR. *Brussels: European Commission* 23 (September): 1–24.

Association for Computing Machinery US Public Policy Council (USACM). 2017. 'Statement on Algorithmic Transparency and Accountability'. *USACM Press Releases*. https://www.acm.org/binaries/content/assets/public-policy/2017_usacm_statement_algorithms.pdf.

Ballard, J.G. 2006. 'The Thousand Dreams of Stellavista (SS)'. *The Complete Short Stories V.1*, 414–36.

Bellotti, Victoria, and Abigail Sellen. 1993. 'Design for Privacy in Ubiquitous Computing Environments'. In *Proceedings of ECSCW '93*, 77–92.

Bier, Henriette, and Terry Knight. 2010. 'Digitally-Driven Architecture'. *Footprint*, no. 6: 1–4.

'BIM Level 2'. 2018. Accessed March 13. http://bim-level2.org/en/standards/.

Bradshaw, Tim. 2018. 'Review: Ember, the "intelligent Cup" for the Smart Home'. *Financial Times*. https://www.ft.com/content/0ca91f5a-205d-11e8-a895-1ba1f72c2c11.

Brand, Stewart. 1995. 'How Buildings Learn: What Happens after They're Built'. *Penguin Books*. doi:10.2307/990971.

Brown, Ian. 2015. 'GSR Discussion Paper Regulation and the Internet of Things'. *International Telecommunications Union*. Geneva.

Bullivant, L. 2006. 'Responsive Environments.' London: Victoria & Albert Museum.

Busta, H. 2017. 'ThyssenKrupp and Microsoft Are Making the Elevator Smart'. *The Architects' Magazine*.

Camp, Jeffrey Van. 2018. ‘The Best Smart Speakers: Alexa, Google Assistant, Siri, Cortana’. *Wired*.

Čas, Johann. 2011. ‘Ubiquitous Computing, Privacy and Data Protection: Options and Limitations to Reconcile the Unprecedented Contradictions’. In *Computers, Privacy and Data Protection: An Element of Choice*, 139–69. Dordrecht: Springer Netherlands. doi:10.1007/978-94-007-0641-5_7.

Clifford, Damian. 2017. ‘Citizen-Consumers in a Personalised Galaxy: Emotion Influenced Decision-Making, a True Path to the Dark Side?’

Colesky, M, J Hoepman, and C Hillen. 2016. ‘Critical Analysis of Privacy Design Strategies’. JOUR. *International Workshop on Privacy Engineering – IWPE’16*, 33–40.

Coletta, Claudio, and Rob Kitchin. 2017. ‘Algorhythmic Governance: Regulating the “heartbeat” of a City Using the Internet of Things’. *Big Data & Society* 4 (2): 205395171774241. doi:10.1177/2053951717742418.

Crabtree, Andy, and Richard Mortier. 2015. ‘Human Data Interaction : Historical Lessons from Social Studies and CSCW’. In *Proceedings of the 2015 14th European Conference on Computer-Supported Cooperative Work, ECSCW’15*, 3–21. doi:10.1007/978-3-319-20499-4.

Crabtree, Andy, and Tom Rodden. 2004. ‘Domestic Routines and Design for the Home’. *Computer Supported Cooperative Work: CSCW: An International Journal* 13 (2): 191–220. doi:10.1023/B:COSU.0000045712.26840.a4.

Crabtree, Andy, Peter Tolmie, and Will Knight. 2017. ‘Repacking “Privacy” for a Networked World’. *Computer Supported Cooperative Work: CSCW: An International Journal* 26 (4–6): 453–88. doi:10.1007/s10606-017-9276-y.

D. Haggerty, Richard V. Ericson, Kevin. 2000. ‘The Surveillant Assemblage’. *British Journal of Sociology* 51 (4): 605–22. doi:10.1080/00071310020015280.

DCMS. 2018. ‘Secure by Design’. https://www.gov.uk/government/publications/secure-by-design.

Deakin, Simon. 2015. ‘The Internet of Things: Shaping Our Future’,. JOUR. Cambridge.

Deleuze, Gilles. 1992. ‘Postscript on the Societies of Control’. *October* 59 (1): 3–7. doi:10.2307/778828.

Department for Business Innovation & Skills, Knowledge Transfer Network, British Standards Institute. 2010. ‘PAS 2016:Next Generation Access for New Build Homes – Guide’.

Dourish, Paul. 2004. ‘Moving Toward Design’. *Where the Action Is:The Foundations of Embodied Interaction*. doi:10.1111/j.1471-1842.2007.00725.x.

Duffy, Francis. 1990. ‘Measuring Building Performance’. *Facilities* 8 (5): 17–20. doi:10.1108/EUM0000000002112.

Edwards, Lilian. 2016. ‘Privacy , Security and Data Protection in Smart Cities: A Critical EU Law Perspective’. *European Data Protection Law Review* 2 (1): 28–58. doi:10.5281/zenodo.34501.

Edwards, Lilian, and Michael Veale. 2017. ‘Slave to the Algorithm? Why a Right to Explanationn Is Probably Not the Remedy You Are Looking for’. *SSRN Electronic Journal*. doi:10.2139/ssrn.2972855.

Eng, Kynan, Andreas Baebler, Ulysses Bernardet, Mark Blanchard, Marcio Costa, Tobi Delbrück, R.J. J Douglas, et al. 2003. ‘Ada - Intelligent Space: An Artificial Creature for the Swiss Expo.02’. In *IEEE International Conference on Robotics and Automation ICRA 2003*, 3:4154–59. doi:10.1109/ROBOT.2003.1242236.

Floridi, Sandra Wachter Brent Mittelstadt Luciano. 2017. ‘Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection

Regulation'. *International Data Privacy Law* 7 (2): 76–99.
Fox, Michael, and Miles Kemp. 2009. 'Interactive Architecture'. In , 256. Princeton Architectural Press.
Frazer, J. H. 2001. 'The Cybernetics of Architecture: A Tribute to the Contribution of Gordon Pask.' *Kybernetes* 30 (5–6): 641–651.
Friedman, Batya, Peter H Kahn, and Alan Borning. 2008. 'Value Sensitive Design and Information Systems'. In *The Handbook of Information and Computer Ethics*, edited by K Himma and H Tavani. New York: Wiley and Sons.
Gaffney, Christopher, and Cerianne Robertson. 2016. 'Smarter than Smart: Rio de Janeiro's Flawed Emergence as a Smart City'. *Journal of Urban Technology*, April. Routledge, 1–18. doi:10.1080/10630732.2015.1102423.
Glasgow City Council. 2013. 'Glasgow Wins £24 Million Future Cities Competition'. *Glasgow.gov.uk*. https://www.glasgow.gov.uk/index.aspx?articleid=9647.
Glynn, Rauiri. 2005. 'Reciprocal Space'. http://www.interactivearchitecture.org/reciprocal-space-ruairi-glynn.html.
Graham, Stephen. 2009. 'Cities as Battlespace: The New Military Urbanism'. *City* 13 (4). Routledge : 383–402. doi:10.1080/13604810903298425.
Green, Keith Evan. 2016. *Architectural Robotics: Ecosystems of Bits, Bytes, and Biology*.
Greenberg, Andy. 2017. 'The Reaper Botnet Could Be Worse Than the Internet-Shaking Mirai Ever Was'. *Wired*. https://www.wired.com/story/reaper-iot-botnet-infected-million-networks/.
Griffiths, Hannah. 2017. 'The Future of Street Lighting'. London.
Guerra, I., F. Borges, J. Padrão, J. Tavares, and M.H. Padrão. 2017. 'Smart Cities, Smart Tourism? The Case Of The City Of Porto'. *Revista Galega de Economía* 26 (2). University of Santiago de Compostela. Faculty of Economics and Business.: 129–42.
Guidotti, Riccardo, Anna Monreale, Franco Turini, Fosca Giannotti, and Dino Pedreschi. 2018. 'A Survey Of Methods For Explaining Black Box Models'.
Hadar, Irit, Tomer Hasson, Oshrat Ayalon, Eran Toch, Michael Birnhack, Sofia Sherman, and Arod Balissa. 2017. 'Privacy by Designers: Software Developers' Privacy Mindset'. *Empirical Software Engineering*, April. Springer US, 1–31. doi:10.1007/s10664-017-9517-1.
Hautala, Laura. 2017. 'Smart Toy Flaws Make Hacking Kids' Info Child's Play'. *CNET*. https://www.cnet.com/uk/news/cloudpets-iot-smart-toy-flaws-hacking-kids-info-children-cybersecurity/.
Hecht, Howard, Mahemuti Mayier, and Christine Perakslis. 2014. 'Pervasive Connectivity: The Thriving Hotel of the Future'. In *2014 IEEE International Conference on Pervasive Computing and Communication Workshops, PERCOM WORKSHOPS 2014*, 357–63. doi:10.1109/PerComW.2014.6815232.
HM Government. 2016. *The Building Regulations 2010 - R1 In-Building Physical Infrastructure APPROVED DOCUMENT R Physical Infrastructure for High-Speed Electronic Communications Networks*.
IBM. 2011. 'Glasgow Named an IBM Smarter City'. *IBM News Room*. https://www-03.ibm.com/press/uk/en/pressrelease/33994.wss.
IEEE. 2016. 'Ethically Aligned Design: A Vision for Prioritising Human Wellbeing with Artificial Intelligence and Autonomous Systems'.
IET. 2017. 'How to Become a Smart Home Installer'. *The Institute of Engineering & Technology*. https://electrical.theiet.org/wiring-matters/issues/65/how-to-become-a-smart-home-installer/.
Innovate UK. 2016. 'Launch of Digital Built Britain'. *Gov.uk*.

https://www.gov.uk/government/news/launch-of-digital-built-britain.
Innovate UK & Infrastructure / Project Authority. 2017. 'Creating a Digital Built Britain: What You Need to Know'. *Gov.uk*. https://www.gov.uk/guidance/creating-a-digital-built-britain-what-you-need-to-know.
Jäger, Nils, Holger Schnädelbach, and Jonathan Hale. 2016. 'Embodied Interactions with Adaptive Architecture'. In *Architecture and Interaction: Human Computer Interaction in Space and Place*, 183–202. doi:10.1007/978-3-319-30028-3_9.
Jäger, Nils, Holger Schnädelbach, Jonathan Hale, David Kirk, and Kevin Glover. 2017. 'Reciprocal Control in Adaptive Environments'. *Interacting with Computers* 29 (4): 512–29. doi:10.1093/iwc/iww037.
JM Porip. 2016. 'How to Search the Internet of Things for Photos of Sleeping Babies | Ars Te'. *Ars Technica*.
Jones, Simon, Sukhvinder Hara, and Juan Carlos Augusto. 2015. 'eFRIEND: An Ethical Framework for Intelligent Environments Development'. *Ethics and Information Technology* 17 (1): 11–25. doi:10.1007/s10676-014-9358-1.
Khan, Omar. 2010. 'Open Columns : A Carbon Dioxide (CO2) Responsive Architecture'. *ACM CHI*, 4789–92. doi:10.1145/1753846.1754232.
Kitchin, Rob. 2014. 'The Real-Time City? Big Data and Smart Urbanism'. *GeoJournal*. Springer Verlag.
———. 2015. 'The Promise and Perils of Smart Cities'. *Computers & Law* 26 (2).
Kitchin, Rob, and Martin Dodge. 2011. *Code / Space: Software and Everyday Life*. *MIT Press*. MIT. doi:10.1080/00343404.2012.696477.
Klauser, Francisco, Till Paasche, and Ola Söderström. 2014. 'Michel Foucault and the Smart City: Power Dynamics Inherent in Contemporary Governing through Code'. *Environment and Planning D: Society and Space* 32 (5). SAGE PublicationsSage UK: London, England: 869–85. doi:10.1068/d13041p.
Kolarevic, Branko, and Vera. Parlac. n.d. *Building Dynamics : Exploring Architecture of Change*. Routledge.
Kroll, Joshua, Joanna Huey, Solon Barocas, Edward Felten, Joel Reidenberg, David Robinson, and Harlan Yu. 2017. 'Accountable Algorithms'. *University of Pennsylvania Law Review* 165 (3).
Kronenburg, Robert. 2012. *Portable Architecture*.
Langheinrich, Marc. 2001. 'Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems'. In *3rd International Conference on Ubiquitous Computing*, 273–91.
Latour, Bruno. 1992. '"'Where Are the Missing Masses? The Sociology of a Few Mundane Artifacts"'. In *Shaping Technology /Building Society*, edited by Weibke Bijker and John Law, 205–24. Cambridge, MA: MIT Press.
Lehikoinen, Juha, and Ville Koistinen. 2014. 'In Big Data We Trust?' *Interactions* 21 (5): 38–41. doi:10.1145/2641398.
Leppënen, Sanna, and Marika Jokinen. 2003. 'Daily Routines and Means of Communication in a Smart Home'. JOUR. In *Inside the Smart Home*, edited by Richard Harper, 207–25. London: Springer Verlag. doi:10.1007/1-85233-854-7_11.
Lessig, L. 2006. *Code Version 2.0*. JOUR. *0 Basic Books New York*. Basic Books, New York.
Lessig, Lawrence. 1999. *Code and Other Laws of Cyberspace*. New York: Basic Books.
Leverett, Eireann, Richard Clayton, and Ross Anderson. 2017. 'Standardisation and Certification of the 'Internet of Things'. *Proceedings of WEIS*, 1–24.
Leyden, John. 2017. 'Another IoT Botnet Has Been Found Feasting on Vulnerable IP Cameras • The Register'. *The Register*. https://www.theregister.co.uk/2017/05/10/persirai_iot_botnet/.

Luger, E., L. Urquhart, T. Rodden, and M. Golembewski. 2015. ‘Playing the Legal Card: Using Ideation Cards to Raise Data Protection Issues within the Design Process’. In *Conference on Human Factors in Computing Systems - Proceedings*. Vol. 2015–April. doi:10.1145/2702123.2702142.

Luger, Ewa, Stuart Moran, and Tom Rodden. 2013. ‘Consent for All’. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI ’13*, 2687. New York, New York, USA: ACM Press. doi:10.1145/2470654.2481371.

Lyon, David. 2003. *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. New York: Routledge.

Mäkinen, Liisa A. 2016. ‘Surveillance On/Off: Examining Home Surveillance System’s From the User’s Perspective’. *Surveillance and Society* 14 (1): 59–77.

Mangiaracina, Riccardo, Alessandro Perego, Giulio Salvadori, and Angela Tumino. 2017. ‘A Comprehensive View of Intelligent Transport Systems for Urban Smart Mobility’. *International Journal of Logistics Research and Applications* 20 (1). Taylor & Francis: 39–52. doi:10.1080/13675567.2016.1241220.

Mathews, S. 2006. ‘The Fun Palace as Virtual Architecture: Cedric Price and the Practices of Indeterminacy’. *Journal of Architectural Education.*

McStay, Andrew. 2016. ‘Empathic Media and Advertising: Industry, Policy, Legal and Citizen Perspectives (the Case for Intimacy)’. *Big Data & Society* 3 (2): 205395171666686. doi:10.1177/2053951716666868.

———. 2017. ‘An Ethical Intervention into Conscious Cities’. *Conscious Cities* 3 (July): 205395171666686. doi:10.1177/2053951716666868.

McStay, Andy. 2017. ‘Tech Firms Want to Detect Your Emotions and Expressions, but People Don’t like It’. *The Conversation*. https://theconversation.com/tech-firms-want-to-detect-your-emotions-and-expressions-but-people-dont-like-it-80153.

Moran, Stuart, Nils Jäger, Holger Schnädelbach, and Kevin Glover. 2016. ‘ExoPranayama: A Biofeedback-Driven Actuated Environment for Supporting Yoga Breathing Practices’. *Personal and Ubiquitous Computing* 20 (2): 261–75. doi:10.1007/s00779-016-0910-3.

Mozer, Michael C. 2005. ‘Lessons from an Adaptive Home’. In *Smart Environments*, 271–94. Hoboken, NJ, USA: John Wiley & Sons, Inc. doi:10.1002/047168659X.ch12.

Murakami Wood, David. 2015. ‘Smart City, Surveillance City’. *Computers and Law*. https://www.scl.org/articles/3405-smart-city-surveillance-city.

Nagenborg, Michael, Anders Albrechtslund, Martin Klamt, David Murakami Wood, Rafael Capurro, Johannes Britz, Thomas Hausmanninger, Makoto Nakada, and Felix Weil. 2010. ‘ICT & The City’. *International Review of Information Ethics* 12 (1203).

Narayanan, Arvind, and Vitaly Shmatikov. 2008. ‘Robust de-Anonymization of Large Sparse Datasets’. In *Proceedings - IEEE Symposium on Security and Privacy*, 111–25. doi:10.1109/SP.2008.33.

Neyland, Daniel, and Norma Möllers. 2017. ‘Algorithmic IF … THEN Rules and the Conditions and Consequences of Power’. *Information Communication and Society* 20 (1): 45–62. doi:10.1080/1369118X.2016.1156141.

NHBC Foundation. 2016. ‘The Connected Home’. Milton Keynes.

Nijholt, Anton, Job Zwiers, and Jan Peciva. 2009. ‘Mixed Reality Participants in Smart Meeting Rooms and Smart Home Environments’. *Personal and Ubiquitous Computing* 13 (1): 85–94. doi:10.1007/s00779-007-0168-x.

Nissenbaum, Helen. 2009. *Privacy In Context: Technology Policy And The Integrity Of Social Life*. Stanford Law Books. doi:10.1207/S15327051HCI16234_03.

Norris, Clive, and Michael McCahill. 2006. ‘CCTV: Beyond Penal Modernism?’ *British Journal of Criminology* 46 (1): 97–118. doi:10.1093/bjc/azi047.

Ofcom. 2017. ‘Connected Nations 2017’. *Ofcom*.

Paine, R. T. 1981. *The Art and Architecture of Japan*. Yale University Press.

Pardes, Arielle. 2017. ‘Nest Cam IQ: Specs, Price, Release Date’. *Wired*. https://www.wired.com/2017/05/nest-cam-iq/.

Picard, Rosalind W. 2000. *Affective Computing*. MIT Press.

Randall, Tom. 2015. ‘The Edge Is the Greenest, Most Intelligent Building in the World’. *Bloomberg Businessweek*. https://www.bloomberg.com/features/2015-the-edge-the-worlds-greenest-building/.

Reidenberg, J. 1998. ‘Lex Informatica: The Formulation of Policy Rules through Technology’. JOUR. *Texas Law Review* 76: 553.

Rodden, Tom, and Steve Benford. 2003. ‘The Evolution of Buildings and Implications for the Design of Ubiquitous Domestic Environments’. In *Proceedings of the Conference on Human Factors in Computing Systems - CHI ’03*, 9. doi:10.1145/642611.642615.

Rose, Karen, Scott Eldridge, and Lyman Chapin. 2015. ‘Internet of Things: An Overview’. *Geneva: Internet Society*.

SATORI Project. 2017. ‘Outline of an Ethics Assessment Framework’.

Schnädelbach, H., Glover, K., & Irune, A. A. 2010. ‘ExoBuilding: Breathing Life into Architecture’. *Conference on Computer-Human Interaction, Reykjavik.*, 442–51. doi:http://doi.org/10.1145/1868914.1868965.

Schnädelbach, H., Irune, A., Kirk, D., Glover, K. and Brundell, P. 2012. ‘ExoBuilding: Physiologically Driven Adaptive Architecture’. *ACM Transactions in Computer Human Interaction (TOCHI)* 19 (4).

Schnädelbach, H. 2016. ‘Conceptual Framework of Adaptive Architecture’.

Schnädelbach, H., N. Jäger, N. Dalton, D. Kirk, S. Nabil, and E. Churchill. 2017. ‘People, Personal Data and the Built Environment’. *DIS 2017 Companion - Proceedings of the 2017 ACM Conference on Designing Interactive Systems*, 360–63. doi:10.1145/3064857.3064864.

Schnadelbach, H, N Jager, and L Urquhart. 2018. ‘Adaptive Buildings and Personal Data’. Under Review. Nottingham.

Schnädelbach, Holger. 2010. ‘Adaptive Architecture-A Conceptual Framework’. In *Media City: Interaction of Architecture, Media and Social Phenomena*, 523–556. Weimar.

Scottish Government. 2015. ‘Building Standards Review 2015 - 4.14 In-Building Physical Infrastructure for High-Speed Electronic Communications Network’.

Selbst, Andrew D, and Solon Barocas. 2017. ‘Regulating Inscrutable Systems’. In *WeRobot 2017*.

Selbst, Andrew, and Julia Powles. 2017. ‘Meaningful Information and the Right to Explanation’.

Selinger, Michelle, and Tony Kim. 2015. ‘Smart City Needs Smart People: Songdo and Smart + Connected Learning’. In *Smart Cities as Democratic Ecologies*, 159–72. London: Palgrave Macmillan UK. doi:10.1057/9781137377203_11.

Sengers, Phoebe, Kirsten Boehner, Shay David, and Joseph ‘Jofish’ Kaye. 2005. ‘Reflective Design’. In *Proceedings of the 4th Decennial Conference on Critical Computing: Between Sense and Sensibility*, 49–58. doi:10.1145/1094562.1094569.

Simmonds, Ian, and David Ing. 2000. ‘A Shearing Layers Approach to Information Systems Development’. *THE STRUCTURE OF ILL-STRUCTURE SOLUTIONS: BOUNDARY OBJECTS AMD HETEROGENEOUS DISTRIBUTED ARTIFICIAL*

INTELLIGENCE. IN M. HUHNS AND L. GASSER EDITORS. DISTRIBUTED ARTIFICIAL INTELLIGENCE 2, 37--54.

Smaniotto, Carlos, Costa | Chair, and Ficha Técnica. 2017. *THE MAKING OF THE MEDIATED PUBLIC SPACE Essays on Emerging Urban Phenomena*.

Somnox. 2018. 'Somnox World's First Sleep Robot - Better Sleep Is Here'. https://www.somnox.nl/.

Spiekermann, S., and F. Pallas. 2006. 'Technology Paternalism – Wider Implications of Ubiquitous Computing'. *Poiesis & Praxis* 4 (1). Springer Berlin Heidelberg: 6–18. doi:10.1007/s10202-005-0010-3.

Stahl, Bernd Carsten, Grace Eden, and Marina Jirotka. 2013. 'Responsible Research and Innovation in Information and Communication Technology: Identifying and Engaging with the Ethical Implications of ICTs'. In *Responsible Innovation: Managing the Responsible Emergence of Science and Innovation in Society*, 199–218. doi:10.1002/9781118551424.ch11.

Thomas, Vanessa, Ding Wang, Louise Mullagh, and Nick Dunn. 2016. 'Where's Wally? In Search of Citizen Perspectives on the Smart City'. *Sustainability (Switzerland)* 8 (3). doi:10.3390/su8030207.

Thorns, Ella. 2018. 'Living Architecture "Astrocyte" Questions Whether Buildings Can Think and Care'. *ArchDaily*. ArchDaily.

Tieman, Ross. 2017. 'Barcelona: Smart City Revolution in Progress'. *Financial Times*. https://www.ft.com/content/6d2fe2a8-722c-11e7-93ff-99f383b09ff9.

Tolmie, Peter, Andy Crabtree, Stefan Egglestone, Jan Humble, Chris Greenhalgh, and Tom Rodden. 2010. 'Digital Plumbing: The Mundane Work of Deploying UbiComp in the Home'. *Personal and Ubiquitous Computing* 14 (3). Springer-Verlag: 181–96. doi:10.1007/s00779-009-0260-5.

Tolmie, Peter, James Pycock, Tim Diggins, Allan MacLean, and Alain Karsenty. 2002. 'Unremarkable Computing'. *Computer-Human Interaction (CHI) Conference 2002* 1 (1): 399–406. doi:10.1145/503447.503448.

UK Information Commissioner Office. 2017. 'Big Data, Artificial Intelligence, Machine Learning and Data Protection'. Wilmslow.

Urquhart, Lachlan. 2017. 'Ethical Dimensions of User Centric Regulation.' *ORBIT Journal* 1 (1): 17. doi:10.29297/orbit.v1i1.14.

Urquhart, Lachlan, and Derek McAuley. 2018. 'Avoiding the Internet of Insecure Industrial Things'. *Computer Law & Security Review*, January. doi:10.1016/j.clsr.2017.12.004.

Urquhart, Lachlan, and Tom Rodden. 2017. 'New Directions in Information Technology Law: Learning from Human–computer Interaction'. *International Review of Law, Computers & Technology* 31 (2): 150–69. doi:10.1080/13600869.2017.1298501.

Urquhart, Lachlan, Neelima Sailaja, and Derek McAuley. 2017. 'Realising the Right to Data Portability for the Domestic Internet of Things'. *Personal and Ubiquitous Computing*, August 23. doi:10.1007/s00779-017-1069-2.

Varshney, Upkar. 2007. 'Pervasive Healthcare and Wireless Health Monitoring'. *Mobile Networks and Applications* 12 (2–3): 113–27. doi:10.1007/s11036-007-0017-1.

Verbeek, P.-P. 2006. 'Materializing Morality: Design Ethics and Technological Mediation'. *Science, Technology & Human Values* 31 (3): 361–80. doi:10.1177/0162243905285847.

Verbeek, PP. 2017. 'BRIdging Data in the Built Environment (BRIDE)'. Twente.

Weber, Rolf H. 2015. 'Internet of Things: Privacy Issues Revisited'. *Computer Law & Security Review* 31 (5): 618–27. doi:10.1016/j.clsr.2015.07.002.

Webster, C. William R., and Charles Leleux. 2018. 'Smart Governance: Opportunities

for Technologically-Mediated Citizen Co-Production'. *Information Polity* 23 (1): 95–110. doi:10.3233/IP-170065.

Weiser, Mark. 1991. 'The Computer for the 21st Century'. *Scientific American* 1 (1): 19–25.

Wiener, Norbert. 1948. *Cybernetics, or Control and Communication in the Animal and the Machine.* Cambridge: MIT Press.

Wilson, C. 2015. 'Smart Homes and Their Users: Analysis and Key Challenges'. JOUR. *Personal and Ubiquitous Computing* 19: 463–76.

Wilson, Peter. 2008. 'Jubilee Campus, Nottingham by Make'. *The Architects' Journal*. https://www.architectsjournal.co.uk/jubilee-campus-nottingham-by-make/1885933.article.

Winner, Langdon. 1986. 'Do Artefacts Have Politics?' *The Whale and the Reactor. A Search for Limits in an Age of High Technology*, 19–39. doi:10.2307/20024652.

Yang, Rayoung, and Mark W Newman. 2013. 'Learning from a Learning Thermostat'. In *Proceedings of the 2013 ACM International Joint Conference on Pervasive and Ubiquitous Computing - UbiComp '13*, 93. doi:10.1145/2493432.2493489.

Appendix 1: Breakdown of A29 WP Allocation of Responsibilities to IoT stakeholders.

Actors	Responses
All[3]	○ Conduct **privacy impact assessments** (PIAs) prior to releasing new applications (share publicly where possible).[4] ○ If using **raw personal data** is being used, delete quickly after use. ○ Create **'user friendly' methods** for interacting around consent, rights to refusing processing and when providing information. ○ **Provide users with more control over their data**[5] ○ Broadly apply the principles of **Privacy by Design and by Default.**
Operating Systems & Device Manufacturers[6]	○ Comply with **'security by design'** ideals e.g. encryption, '*provide simple tools to notify users and update devices when security vulnerabilities are found*'. ○ **Increase information available to users** around type, time and frequency of data collection, including providing a '**do not disturb' type function** that has timed disabling of sensors. ○ **Provide tools to allow users to locally read, modify and edit data** (which will be in an interoperable/portable format) before it travels to any other data controllers in the network. ○ For shared devices: "*A setting should be available to distinguish between different individuals using the same device so that they cannot learn about each other's' activities*."[7]
IoT Device Owners and Additional Recipients of data[8]	○ Let **non-user data subjects know about any IoT data collection related to them** and respect their wishes of they don't want their data to be collected.
Standardisation bodies & Data Platforms[9]	○ Promote **portable, interoperable, clear data formats** that enable easy transfers and support user understanding of sharing. ○ **Certify baseline standards** around users' security and privacy ○ Create "*lightweight encryption and communication protocols adapted to the specificities of IoT, guaranteeing confidentially, integrity, authentication and access control*".[10]
Social Platform	○ Social platform[11] applications based on IoT devices need to **let users edit and review information before it is shared on social networks**. ○ Default for any information published on such platforms should be to "*not become public or be indexed by search engines*".
Application Developers	○ **Aggregated data should be used where possible**, instead of raw personal data ○ Incorporate **frequent notices and warnings in systems** to remind users of sensor data collection.

[3] Section 7.1
[4] Drawing on the 2011 RFID PIA Framework as a reference point
[5] According to the principle of self-determination of data
[6] Section 6.1
[7] Section 6.1 p23
[8] Section 6.4
[9] Section 6.5
[10] Section 6.5
[11] Section 6.3