Sophia Maalsen
The University of Sydney, Australia
sophia.maalsen@sydney.edu.au

Jathan Sadowski
The University of Sydney, Australia
jathan.sadowski@sydney.edu.au

Abstract

Some of the largest tech companies in the world, not to mention a stream of smaller startups, are now our roommates. Homes have become the target for smart devices and digital platforms that aim to upgrade old appliances, like refrigerators, and provide new capabilities, like virtual assistants. While smart devices have been variously championed and demonized in both academic literature and popular media, this article moves critical analysis beyond the common—but still important—concerns with privacy and security. By directing our attention to the wider political economy of datafication, it reveals the increasingly influential, yet shadowy, role of industries outside the tech sector in designing and deploying surveillance systems in domestic spaces. Namely, the FIRE sector of finance, insurance, and real estate. When Amazon and Google moved into our homes, they also let in a suite of uninvited third parties.

“In short, the home is becoming a data factory.”
— Justin McGuirk (2015)

Introduction

The “smart home” has represented a persistent vision of utopian domestic futures since at least the mid-twentieth century. Although the vision has had many iterations, from the space age hypermodern home of the 1950s, to the home-as-computer of the 1980s and 90s, they all remain a variation on a theme: home automation will reduce the amount of housework, improve resource efficiency, increase leisure time, and turn our homes into fortified castles with surveillance and security systems (Nicholls et al. 2017; Darby, 2017; Strengers 2013; Strengers and Nicholls 2017). Recent incarnations of the smart home have been augmented by the Internet of Things (IoT), which allows connected devices to collect data on household practices, communicate with cloud platforms, coordinate with other devices, control parts of the home, and provide real-time feedback to users, manufacturers, and third parties (Gram-Hanssen and Darby 2018; Hargreaves et al. 2017; Strengers et al. 2016).

This model of contemporary living has been variously championed and demonized in both the academic literature and popular media. By analyzing the occupant’s behavior and preferences, the smart house is meant to be equipped with responsive and predictive capabilities that make daily life more convenient and comfortable. But these same capabilities have raised privacy and security concerns, with critics pointing out how smart devices make us vulnerable to spying and hacking by corporations, governments, and black hats (Apthorpe et al. 2017).
While these points are important, grappling with the scale, impact, and trajectory of the integration of networked devices and digital platforms into our homes requires looking beyond common celebrations and criticisms. We have to do more than ask procedural questions about the smart home: Are data streams anonymized and aggregated? Are internet connections encrypted? Are automated systems accurate? We must also pose political economic questions about whose interests and what logics are materialized by the smart home. When some of the largest companies in the world, not to mention a host of smaller startups, are now our roommates, it is not enough to call them “creepy,” especially when they demonstrate paternalistic tendencies.

The digital collection and production of data has altered focus from the individual as a subject of discipline to the modulated “dividual”: beings divided into any number of pieces that are separated, scrutinized, and distributed across databanks (Deleuze 1992). Smart systems, many have argued, have shifted society from one of discipline to one of control (Gabrys 2014; Sadowski and Pasquale 2015). Yet, at the same time, it is important to recognize that these different power relations are not exclusive but rather overlapping, coproduced, and context dependent—the individual can be reassembled from its dividual form (Iveson and Maalsen 2018; Evans and Kitchin 2018). The simultaneous transition to control and the intensification of discipline has significant implications for the use of data-driven, networked, automated domestic environments to mold and modulate our behavior, turning us into good occupants of smart homes.

In this article, we cast light on the increasingly influential, yet shadowy role of industries other than the tech sector in designing and deploying surveillance systems in domestic spaces. We focus, particularly, on the FIRE sector—finance, insurance, and real estate—which is embracing the power of smart homes as a means to advance their own ends at the expense of our private domestic lives.

Home Invasion

While used as a readymade argument against intrusion and interference, the cliché that you have the right to do X “in the privacy of your own home” has never been universally applied. The private and public spheres are not necessarily separated by the threshold of our homes. For some, this is a solid boundary but for others it has always been more like a porous membrane that allows outsiders to monitor what people do and manage how people live inside their homes. As this section illustrates, the division between boundary and membrane has tended to fall along familiar categories: rich and poor, men and women, white and people of color.

Digital platforms heighten the ways in which privacy is treated as a premium upgrade. But rather than a disruption, the smart home is an amplification and acceleration of previous forms of domestic discipline. It is worth briefly looking at two examples that set key precedents for smart home surveillance.

First, social welfare programs are one of the main ways disciplinarians have entered the home. In the US, welfare policy has taken a particularly paternalistic and punitive turn since major reforms in the mid-1990s (Schram et al. 2009). Receiving public aid also means adhering to behavioral expectations, being subjected to compliance supervision, and suffering penalties for infractions. Now “welfare programs use a variety of incentives, surveillance mechanisms, and restrictive rules to modify client behaviors” (Schram et al. 2009: 398).

Under the banners of “family values” and “hard work”—two ideals that linked austere neoliberals and social conservatives (Cooper 2017)—the government pried open a window into the private lives of vulnerable groups in society. Yet, domestic discipline is not just limited to the state.

Second, various corporations have an interest in knowing and changing what we do behind closed doors. Perhaps the most obvious example is the consumer credit industry—a close runner-up is marketing—which continues to pioneer intrusive methods for compiling and categorizing personal information (Citron and Pasquale 2014). However, the reasons and techniques for private industry enforcing private value are not
monopolized by credit scorers. A particularly egregious, yet little discussed, example comes from the paragon of twentieth century capitalism: Fordism.

Famously, Ford declared that his factory workers would be paid enough to afford their own Ford car, thus more than doubling the minimum wage at the time. What is not as widely known, though, is that not just anybody was eligible for the increased wage. Just like with government welfare, workers had to meet strict lifestyle and behavioral criteria. As historian Richard Snow reports: “To qualify for his doubled salary, the worker had to be thrifty and continent. He had to keep his home neat and his children healthy, and, if he were below the age of twenty-two, to be married” (2014: 231). To ensure workers met these requirements and were not wasting their new wealth on drinking, gambling, and other vices, Ford created a “Sociological Department” at the company that sent out investigators to workers’ homes. The investigators conducted in-depth questionnaires, made unannounced visits, and advised workers on how to live correctly. The Sociological Department “grew to a force two hundred strong” (Snow 2014: 232). Russian immigrants working for Ford compared his investigators to the czar’s secret police.

Watching people in their homes has always been, first and foremost, a way of exercising power. It might be linked to extracting profit—i.e., living well means working well—but not necessarily. Long before the digital age, government and industry unleashed the disciplinary power of data to track, profile, sort, stratify, score, rank, reward, punish, include, exclude, and otherwise calculate decisions that determine our “life-chances”—the opportunities, pathways, and choices that are open to each of us (Dwyer 2018; Fourcade and Healy 2013). However, within the smart home, the capabilities for disciplinary surveillance, reward, and punishment are accelerated and amplified.

**House FIRE**

Smart devices are not discrete entities, but are connected to broader systems and flows. As Darby (2018: 142) notes with respect to the energy applications of the IoT, the smart home is “not so much a home that is automated for its own sake in order to provide comfort, convenience, and fun, but the home that interacts with electricity networks in order to provide and receive services.” The devices are more than agents that are actively sensing, recording, analyzing, and responding. They are also agents that represent the interests of their makers, communicate with them via the internet, invite them (and maybe their friends) into our homes, and enroll the smart home into a growing network of infrastructure and institutions. Every device and platform installed in the home enlarges the network and multiplies the connections.

Under surveillance capitalism, our devices and appliances are not just commodities, they are also a means of producing data (Sadowski 2019; Zuboff 2015). The “data imperative” (Fourcade and Healy 2017)—which drives organizations to continuously accumulate data—influences the design of household products that are marketed as “new and improved.”

However, while our attention is preoccupied with the usual suspects in Silicon Valley, the smart home has also become a conduit for another dominant sector: FIRE (finance, insurance, and real estate). The power offered by the smart home to monitor households has attracted FIRE companies that have a vested interest in getting to know us better. Simply put, the FIRE sector is based on monetizing information, managing risk, and maintaining assets. Although a simplification of more complex business models, value extraction in all three areas is enabled by collecting data about our domestic actions, habits, and environments, which is used to develop personalized products, services, and incentives that are tailored to shape our behaviors.

This section shows how and why FIRE is getting involved in deploying devices and platforms for the smart home, and what the implications are for those who live in a smart home on FIRE. Due to space constraints and the comparatively much greater amount of critical study “financialization” has garnered over the last ten years (Christophers 2015; Davis and Walsh 2017), we focus here on insurance and real estate.

**Loss Prevention and Control**
The consulting firm AT Kearney (2014) says that smart tech will “disrupt traditional insurance models, while opening new frontiers for growth.” Insurance companies are well aware of this opportunity. On one hand, insurers are partnering with tech firms to offer special deals like discounts on premiums for installing smart home systems and letting them access the data produced. For example, Liberty Mutual, a major American insurer, will even give you a free Nest Protect smoke detector if you let them monitor the device. On the other hand, insurers are also investing in the creation of their own smart tech that is specially designed to collect valuable data. For example, by installing devices like the Progressive “Snapshot” and Admiral “Black Box” in customers’ cars, insurers can monitor how, when, and where each individual drives.

The assistant vice-president of innovation at USAA, Jon-Michael Kowall, told *MIT Technology Review* that he is creating a suite of tech that act like a “check-engine light for the home” (Higginbotham 2016: n.p.). The idea is to fill each customer’s home with sensors that keep track of everything, from leaky pipes to daily routines, and send status reports to the insurance company. They can then use this data to notify customers about potential issues, such as maintenance tasks or even “about whether or not a child made it home from school on time” (Higginbotham 2016: n.p.).

One major insurer uses the jingle, “Like a good neighbor, State Farm is there.” But with the smart home, a more accurate jingle might be, “Like a nosy neighbor, we are always watching.”

Insurers claim that smart devices and data analytics platforms—worn on your body and installed in your home/car—will allow them to charge more accurate prices, thus ensuring that people pay what they should. Their hypothetical examples are always of benefits to customers with unexpected discounts and lower premiums, and that will be true for some people. Yet there is little reason to believe that the industry overall will not use risk scoring, personalized pricing, and other innovations to increase their own revenues. When industries eagerly embrace “disruptive innovation,” it is not because they will be the ones disrupted.

Insurers have always tried to manage risk, not just assess it. The problem comes when the smart home facilitates new methods for squeezing more out of customers and shirking obligations to pay claims.

As insurers act more like platforms that mediate and record everyday life (Srnicek 2017), their calculations about and interventions into our lives become more precise. The CEO of Progressive called the Snapshot a “meaningful start toward personalized insurance pricing based on real–time measurement of your driving behavior—the statistics of one” (Progressive Corporation 2012: 1). Moreover, data monitoring unlocks new abilities for behavioral modification. Through policy conditions and price incentives, insurers can make sure we are all safe bets.

Insurers now offer discounts in return for using certain smart devices and letting them access the data. The tradeoff between dataveillance and discounts can seem innocuous at first, until the data is used to punish and adjust bad behavior. Each node in the networked home can contribute to the insurer’s cost-benefit analysis about you. Driving at the wrong times, procrastinating on home maintenance, watching too much TV, eating unhealthy food—all of these and more can directly impact your insurance policy and premiums (Allen 2018).

The industry euphemism for these practices is “loss prevention and control.” What it really means is shaping people into models of good behavior—or making them pay the price—as defined by insurers. The power that insurers have over the behavior of entire institutions, like multinational corporations and police departments, let alone individuals, has been well documented (Rappaport 2017). “Insurance is one of the greatest sources of regulatory authority over private life” (Baker and Simon 2002: 13). The smart home has the potential to supercharge the insurance industry’s power to surveil, analyze, and discipline.

“In the near future,” Kowall stated, “you’ll give us a mailing address and we will send a box of technology to you. What’s in the box will prevent claims and also offer a better service to policy holders” (Higginbotham 2016: n.p.). Rather than individuals buying upgraded appliances and new gadgets for
themselves, the single biggest driver of smart homes might very well be subsidies from insurers. Indeed, many industry analysts predict that insurance will be a major business model underpinning the IoT, similar to how advertising bankrolls many web platforms now (Myslewski 2014).

This dynamic of reeling people in with short-term benefits (i.e., subsidized devices) and then locking them into long-term exploitation (i.e., intrusive dataveillance) mirrors the process of “predatory inclusion,” wherein financial actors like lenders offer needed products and services to members of marginalized groups “but on exploitative terms that limit or eliminate their long-term benefits” (Seamster and Charron-Chénier 2017: 199). Considering the power of insurers over people’s lives, which is further enhanced by their partnerships with employers (Hull and Pasquale 2018), perhaps their tactics will shift from predatory to mandatory inclusion. The privileged are baited with discounts and gamification into giving up their data, while the vulnerable may be simply coerced into handing over access to private data. Or else they face exclusion from necessary (and legally mandated) insurance.¹

**Digitally Disciplining Tenants**

But it is not just insurers who find value in extracting data from your home—the real estate sector is also heavily invested in knowing about your home habits. The increasing digitalization of the home has much to offer real estate companies and a number of startups are aimed at household management. A key area of intervention is in profiling, rating, and managing occupants of a household, yet the effects of this are experienced unevenly and are predominantly differentiated along lines of home ownership versus rental tenants.

Increasingly, rental tenants are coerced into using platforms for rental applications and payments, which provide a digital record of their behavior as tenants. The controversial rental platform Rentberry supposedly enables the best renting options for both tenants and landlords. Tenants can compete with each other to make the most competitive application by adjusting their bids in relation to other applicants—the details of which are accessed through the site. This means not only offering a competitive rent (i.e., a higher sum than other bids) but building a profile of the applicant as a responsible tenant through the provision of additional details, including rental history, income details, and landlord references. Landlords can outsource background checks on tenants to Rentberry, which offers a service that runs an “extensive check through millions of up to date state and federal records” (Rentberry n.d.), generating detailed credit and personal reports that are sent to the landlords.

Concern has rightly been raised around Rentberry’s encouragement of rent bidding, but the significant amounts of personal data collected by the site should also prompt critique. Those whose profiles are not as competitive—perhaps they did not offer high enough bids or their profile paints them as less responsible tenants—will face more barriers to finding appropriate housing. The longevity of the profile means that this housing insecurity continues to occur into the future. Landlords can then point to data-driven algorithms, not their own biases, as the cause of punishing decisions.

Even less obviously punitive platforms, such as online share housing sites, like flatmates.com.au, require users to create profiles revealing personal data, including age and gender, as well as lifestyle choices. While a user is not compelled to fill out all the details, the logics of the site dictate that success in finding a home correlates with greater amounts of information supplied. This means users can expose details of their sexuality, race, culture, and political choices. Such information may help you choose more appropriate house mates but it can also discriminate, essentialize differences, and reinforce identity tropes (Maalsen 2018; Maalsen and McLean 2016).

Digital intervention also exists within the home. Home finance management apps, such as bill-sharing apps Split Wise and easyshare, make managing household finances easier. This includes the ability to automate calculations and payments, compile a digital record of transactions and, most importantly, create a profile

¹ We thank a reviewer for pointing us to the concept of “predatory inclusion” and raising the possibility of coercion.
of a person’s financial health, which can be used to penalize, incentivize, and shape behavior. Easyshare capitalizes on shifting housing trajectories and the effects that delayed home ownership has on the performance of fiscal responsibility. The declining and delayed rates of home ownership in countries such as Australia, the US, and Ireland means that the usual milestones for credit checks such as a home loans are also delayed. Easyshare frames their service as being able to provide evidence of financial behaviors in the absence of the expected markers of home ownership, which can then be used when applying for loans (Maalsen 2018). Certainly, this can be useful but it also intensifies the gaze on rental tenants, which can have implications for their housing pathways later in life.

People rent rather than own, predominantly, because of financial constraints, such as irregular or lower incomes. The types of apps and platforms described above dictate that any missed payments, online housing profiles, and algorithmic ratings will be recorded for future reference and brought up when they apply for another rental property or are finally in a position to purchase a home. An individual’s digital housing data can affect their ability to be approved for another loan or another rental. Further, these digital judgements are made without reference to an individual’s context and thus reward and penalize unevenly. There are similarities here with Noble’s (2018) observations on digital surveillance as unevenly directed to certain groups based on race, gender, and socio-economic position. The discrimination experienced by these groups is historical and systemic and has structurally affected their housing, employment, credit market, and consumer opportunities, among other social domains (Pager and Shepherd 2008). But the lens of digital surveillance has the potential to exacerbate these discriminatory effects. In the case of rental tenants, surveillance is enabled by platforms because they are in a socio-economic position where they do not have the security of home ownership and loan guarantees. The same platforms then amplify the power that landlords have over the smart home: who gets to live there and who is denied access.

Conclusion

If FIRE does become a major supporter and supplier of the smart home, then what does that mean for how these technologies are developed, how they affect our lives, and who benefits from their use? Each device offers a window into your life, extracting the information needed to mold and modulate your behavior. This has a normative effect on producing “good” household occupants. Every minute you go without replacing the batteries in that chirping Nest Protect can mean added points to your risk score and adjusted premiums. Rental payment platforms may either reward or penalize you, depending on whether you are a “responsible” tenant, regardless of broader contexts and circumstances. The smart home purports to offer a model of efficient living, but if FIRE has its way the “data factory” we live inside will also be used to produce people who conform to its interests. The digital discouragement of deviance and risk exercises modulatory control in the interest of profit, producing a remarkably stale and sterile smart home in the process.

References


