Policing the smart home

Title: Policing the Smart Home: The Internet of Things as 'Invisible Witnesses'.

Authors:

Dr Lachlan Urquhart, Lecturer in Technology Law, School of Law, University of Edinburgh; Visiting Researcher, Horizon Digital Economy Research Institute, School of Computer Science, University of Nottingham. Corresponding Author*

Dr Diana Miranda, Lecturer in Criminology, Faculty of Social Sciences, University of Stirling.

Dr Lena Podoletz, Research Fellow in Emotional AI in Smart Cities, School of Law and School of Informatics, University of Edinburgh.

***Corresponding Author Contact Details:**

School of Law, Old College, South Bridge, Edinburgh, EH8 9YL

lachlan.urquhart@ed.ac.uk

Abstract: In this paper, we develop the concept of smart home devices as 'invisible witnesses' in everyday life. We explore contemporary examples that highlight how smart devices have been used by the police and unpack the socio-technical implications of using these devices in criminal investigations. We draw on several sociological, computing and forensics concepts to develop our argument. We consider the challenges of obtaining and interpreting trace evidence from smart devices; unpack the ways in which these devices are designed to be 'invisible in use'; and consider the processes by which they become domesticated into everyday life. We also analyse the differentiated levels of control occupants have over home devices, and the surveillance impacts of making everyday life visible to third parties, particularly the police.

Key points for practitioners:

1. Traces of interactions in the home can be captured and made visible by Internet of Things (IoT) devices. As they are domesticated into everyday life, they can become 'invisible witnesses', capturing trace evidence of home occupant acts and interactions.

2. IoT devices can create visibility not only of everyday life mundane practices but also of criminal activity involving home occupants.

3. IoT devices enable sensing and inferences that can provide partial stories of what happens in the home. Whilst such forms of trace evidence can shape police narratives during investigations, it is important to recall that homes are complex socio-technical spaces where IoT systems are embedded, controlled, and domesticated in differing ways.

4. Digital forensics processes need to account for the socio-technical challenges posed by internet of things devices being used in investigations.

Keywords: internet of things, smart homes, policing, surveillance.

Word Count: 7855 (including bibliography)

PART 1. Introduction

Recent high-profile news stories of law enforcement agencies seeking access to domestic Internet of Things (IoT) devices have highlighted their growing role in policing. The IoT is enabled through internet connected devices such as smartphones and watches, (Yang et al, 2017) smart televisions, (Malkin et al, 2018) and smart meters (Asghar, 2017) that gather data through ambient sensors e.g., cameras, microphones, accelerometers. IoT devices have limited on board storage capacity, and they largely use cloud storage to store and analyse the sensed data to make inferences about their environment and user e.g., user location, habits, and social networks. As IoT devices become more ubiquitous, they are increasingly domesticated into everyday life (Silverstone et al, 1989; Weiser, 1990). Our analysis frames this shift as leading them to become 'invisible witnesses' that can provide trace evidence of activities in the home. These devices have been sources of trace evidence in criminal investigations of murders, fraud, rape, assault, and arson. Devices ranging from smart speakers, fitness trackers, health apps, and smart water meters have all provided data that shapes police narratives of how these crimes occurred.

Our paper explores the wider socio-technical implications of IoT enabling new forms of longitudinal visibility around everyday life and surveillance of inhabitant routines. In Part 2, we present an overview of what smart homes are and how these systems have been designed to be 'invisible in use' (Weiser, 1990). This helps us to understand the socio-technical significance of bringing smart devices into the home (2.1). We then present a non-exhaustive list of reported examples where police have used IoT data in criminal investigations, highlighting how it factors into their investigative work (2.2). We then introduce Locard's 'exchange principle' (1928) which has traditionally been used to frame how evidence can be gathered in an investigation (2.3). We explore how it applies to different forms of trace

evidence from IoT in the home and the inferences they allow. We then reflect on the practical digital forensics challenges IoT poses for police when gathering data from different types of devices and conclude this section by considering how this changes criminal investigation practices. In Part 3, we consider what it means to live with 'invisible witnesses' in the home, including the surveillance implications of increased visibility and permanent surveillance in these spaces. We particularly focus on the domestication and differentiated levels of control over devices in the home, and the reduction of our backstage due to permanent surveillance (Goffman, 1956) by IoT devices making interactions with users externally visible. In Part 4, we reiterate our 3 key points as our brief conclusions.

PART 2. Setting the (Smart Home) Crime Scene

In this section we focus on how IoT systems are designed, how this shapes their role as 'invisible witnesses', and to unpack the new technical digital forensics' challenges raised.

2.1 Smart Homes, Invisibility and Domestication

Smart homes involve domestic IoT devices and services linked together for 'forms of communication between people and things and among things' (Bhat et al, 2017, p917). As Urquhart, Lodge and Crabtree (2019) state, 'the promise of the IoT is greater convenience, security, safety, efficiency and comfort in a user's everyday life' (p2). IoT devices provide users with contextually appropriate services by collecting data through sensors in the environment, then analysing data to make inferences about occupant behaviour and routines over time. For example, smart fridges and fitness trackers aim to encourage healthier lifestyles by monitoring consumption and activity to prompt healthier lifestyle choices. Unpacking contemporary domestication of IoT into everyday life requires us to briefly consider the history of IoT design and the earlier commitment to a vision of 'invisibility in use'. Back in the early 1990's, Marc Weiser's ubiquitous computing was a key vision of post desktop computing where systems are all around us and "*weave themselves into the fabric of everyday life until*

they are indistinguishable from it" (Weiser, 1990, p94). He inspired others to develop technical infrastructures necessary to realise his vision, such as building 'seamless networking' (i.e., networks that provide constant connectivity) and 'ambient, calm user interfaces' (i.e., ones that are there when needed, but in the background when not). The concept of Ubicomp evolved and new labels emerged, such as pervasive computing (Satyanarayanan, 2001), calm computing (Weiser & Seeley Brown, 1996), ambient intelligence (Aarts and Marzano, 2003), context aware computing (Abowd et al, 1998), and now the Internet of Things (Ashton, 1999). Ultimately, these visions were underpinned by a recurring theme, that of computers 'disappearing' (European Commission/NSF, 2004), becoming 'invisible' (Weiser, 1994) and becoming 'unremarkable in use' (Tolmie et al, 2002).

Whilst technical work had a particular framing of 'invisibility', socio-technical researchers recognised more profound societal shifts beyond clever interface design and networking. Drawing on work of Garfinkel (1967) and Sacks (1992), ethnomethodology researchers understood that embedding technologies into everyday life, to design them to be truly invisible and disappear, required a focus on mundane social practices and the ongoing work of accomplishing technologically mediated routines (Bell & Dourish, 2006; Suchman, 1987; Crabtree, Rouncefield and Tolmie, 2012). Similarly, communications and surveillance studies scholars recognised the links between domestication of technology and everyday life. Silverstone et al (1989) suggest domestication of technology happens when a user is able to '*incorporate and control technological artefacts into [their] own technological culture'* and *'to render them more or less 'invisible' within [their] daily routines*' (p24). Similarly, Lyon has argued, "*computing machinery is embedded, more or less invisibly, in the environments of everyday life*" (Lyon, 2018, p51). Importantly, domestication of technology is not a linear process which stops – instead it is a process where needs, practices, and the environment change with time (Sorensen 1994).

Within smart homes, complex social relations, hierarchies, domestic politics, and power asymmetries are also key to understanding the role of IoT in everyday life (Crabtree & Rodden, 2004). When domesticated and working as intended, these systems are largely invisible to users, making them a form of 'invisible witness'. Smart home user studies highlight how the initial novelty of interfaces like smart thermostats become 'mundane' once these systems integrate into the users' life and work (Yang & Newman, 2013). Pridmore et al (2019) studied implications of intelligent personal assistants (i.e., smart speakers) in 17 focus groups in the US and Netherlands and observed participant concerns about how speakers are 'designed to learn from users' everyday routines and behaviours and integrate into the smart home environment' (p4). For Dutch participants, informational harms were a concern, such as with the ability to monitor behaviours that occur daily and the scope for eavesdropping by external people. For US participants, physical security implications were a greater concern e.g., entering a home due to smart locks being hacked.

We now turn to some examples of recent high-profile news stories to demonstrate how police are using domestic IoT data in criminal investigations.[1] This is not exhaustive but instead provides illustrative examples reported in the press around in the USA, UK, Germany, and Greece. This shows the range of devices and the variety of activities they have been used to make inferences about.

[1] See also Privacy International Resource on this Topic https://privacyinternational.org/long-read/3026/my-fridge-my-witness

2.2 Recent Examples of Police Use of IoT:

USA

- In 2019, Sylvia Galva Crespo was murdered at her home in Florida. An Amazon Echo was believed to hold evidence of audio recordings from an argument prior to the murder (where the device was triggered by its 'wake word' to record the interaction).[2]
- In 2018, the murder of Karen Navarra in San Jose by her stepfather involved Fitbit fitness tracker data that showed a spike and then slow in her heart rate, enabling police to estimate her time of death, coupled with video evidence showing the murderer's car at her house during that time.[3] In the hope of capturing evidence of crimes[4], homeowners with Ring smart doorbells[5] are encouraged to join video sharing networks with US police e.g. Mississippi[6] (and in the UK e.g. Wiltshire[7]).
- In 2017, the double murder case of Christine Sullivan and Jenna Pellagrini in New Hampshire involved the court seeking two days of Amazon Echo recordings to support the case (which Amazon complied with following the court order).[8]
- In 2017, heart rate data from a pacemaker assisted in charges against Ross Compton for arson and insurance fraud in Ohio, despite claims his house fire was accidental[9].

[2] https://amp.theguardian.com/us-news/2019/nov/01/alexa-florida-death-witness-amazon-echo?CMP=Share_AndroidApp_Tweet&__twitter_impression=true
[3] https://www.bbc.co.uk/news/technology-45745366
[4] Recent UK case law suggests homeowners can face data protection compliance obligations and fines when operating home security cameras if they intrude into a neighbours' domestic space (e.g., Fairhurst v Woodard 2021, Oxford County Court G00MK161. See also Urquhart & Chen, 2021.
[5] https://www.vice.com/en/article/zmjp53/how-ring-went-from-shark-tank-reject-to-americas-scariest-surveillance-company
[6] https://www.bbc.co.uk/news/technology-54809228
[7] https://www.bbc.co.uk/news/amp/uk-england-wiltshire-52066945?__twitter_impression=true
[8] https://www.independent.co.uk/life-style/gadgets-and-tech/news/amazon-echo-alexa-evidence-murder-case-a8633551.html
[9] https://www.theguardian.com/technology/2017/jun/23/smart-devices-solve-crime-murder-internet-of-things

- In the 2015, 'hot tub' murder case in Arkansas, Amazon Echo and smart water meters helped solve the murder of Victor Collins.[10] Here the police sought data collected by an Amazon's Echo speaker[11] that was present where the body was found. Following a lawful search warrant, Amazon supplied information from the smart speaker. Other smart home devices were available in that residence including a Nest thermostat, a Honeywell alarm system with door monitoring alarms and motion sensor, and a smart water meter. The latter showed that the quantity of water used when the alleged killing occurred was higher than normal usage which lead the police to believe that it was used to wash away evidence at the crime scene.
- The murder of Connie Dabate in Connecticut in 2015 is one of the earlier cases to use smart device data in 2015. The Fitbit data contradicted witness testimony regarding the time of the crime and it being an alleged home invasion. The data showed that the victim was moving around an hour after the sole witness claimed the murder took place.[12] This was not used as sole evidence for guilt but to justify further questions and support the narrative uncovered by the investigation.

Europe

- In 2021, Caroline Crouch was murdered by her partner in Greece. He created a false narrative about a robbery that was disproved due to inconsistencies between his statement and a combination of data provided by the victim's smart watch, the couple's home surveillance system and perpetrator's mobile phone data.[13] This shows how diverse devices can be 'invisible witnesses' to different parts of the narrative.

[10] https://www.cnet.com/news/police-request-echo-recordings-for-homicide-investigation/ and
[11] http://www.bbc.co.uk/news/technology-39191056
[12] http://www.thedrum.com/news/2017/04/26/fitbit-data-incriminates-man-accused-killing-his-wife
[13] https://www.bbc.co.uk/news/world-europe-57570042

- In the UK in 2018, the case of Jessica Patel's murder through injection of insulin and strangulation by her husband turned on the basis of iPhone health App data. It showed the murderer's narrative of an alleged burglary was false and he was shown to be running around the house to give the appearance of a robbery. His wife's app also showed movement of her corpse by the husband.
- In 2018 in Germany, Apple Health app data contributed to the conviction of Maria Ladenburger's murderer / rapist by suggesting his activity at key time frames i.e., his app showed him 'climbing steps' in the middle of the night, which was interpreted by police as him climbing a river bank to drown his victim. [14]

These cases highlight the role of smart homes and IoT in policing and show how data from these devices was used to counter testimonies from people, to make inferences about actions and intent, and to build the overall narrative of the case. We now turn to the emergent role of IoT 'trace evidence' within criminal investigations.

[14] https://nakedsecurity.sophos.com/2018/01/15/iphones-apple-health-data-used-as-evidence-in-murder-trial/

2.3 IoT Traces and Digital Forensics

Traditionally, crime scene examination requires application of different forensic techniques to enable the recognition, collection, and preservation of physical evidence. Succinctly viewed as 'every contact leaves a trace', Locard's (1928) *Exchange Principle* has long described the process of collection and interpretation of physical evidence e.g. fingerprints left at the crime scene. This principle assumes any contact and interaction between the victim, suspect, and crime scene involves an exchange of material (Locard, 1928). These different physical traces are commonly portrayed as 'silent witnesses' (Kirk, 1974, p2) at the crime scene.

This narrative of 'exchange' and 'witnesses' translates to digital forensics too (Reedy, 2021, p139; Zatyko & Bay, 2014). For example, Akinbi and Berry (2020, p271) state apps integrated with Google Assistant can be a "*silent witness to a crime*" and facilitate a criminal investigation. IoT devices enable traces of offline activities from the physical environment they operate in. This could include inferences about device and user location (via GPS, MAC Address or cell data), frequency of user movements (via accelerometers, cameras, or movement sensors) and duration and type of physical activities (via use logs, data consumption, timestamps of pings between devices and routers/servers). Christenson, Oleson and Sørenson (2021) discuss the importance of IoT devices enabling markers of 'normal behaviour', and being able to establish deviations from normality i.e., "each sensor serves not only to facilitate the little things that they help us with; it serves first and foremost to help the companies behind the devices infer what constitutes normal, routine activities in our homes" (p242). For police investigations, deviations from routine activities can help to construct case narratives e.g., use of excess volumes of water consumed in the middle of the night in the Amazon Echo murder case.

Digital forensics are playing an increasingly important role in investigations (House of Lords, 2019 as cited in Muir & Walcott, 2021). For example, in September 2020 the Director of Public Prosecutions in England and Wales stated smart home devices, such as smart doorbells, Alexa and Siri have provided valuable evidence.[15] However, despite the growing role of digital forensics labs analysing IoT devices and metadata (Casey, Katz & Lewthwaite, 2013; Wilson-Kovacs, 2020), the UK lacks a "standard national competency framework for digital forensic skills" and it needs greater consistency amongst police forces (Wilson-Kovacs, Rappert & Redfern, 2021). Concerningly, a recent small-scale study indicated that digital forensics can be prone to bias and the reliability of the observations, interpretations and conclusions of examiners can be low (Sunde & Dror, 2021). Given the centrality of inferences for interpreting IoT traces, this demonstrates need to develop capacity in digital forensics for IoT. The policy landscape is changing here, and in response to criticism from the UK Information Commissioner Office on police compliance with the UK Data Protection Act 2018 when extracting data from mobile devices,[16] the UK College of Policing has recently released guidance on how to extract data from a range of digital devices and sets standards on best, legally compliant practice.[17]

To support development of better practice around digital forensics with IoT trace data, we now reflect on some priority areas:

Comprehensiveness of data: Digital traces that can be uncovered from smart home IoT devices are often not comprehensive and tell a partial story due to the nature of sensors focused on specific applications e.g., microphones only collecting voice data from smart speakers. As with traditional devices, users can delete data or can otherwise try to make them impossible to

[15] https://www.cps.gov.uk/cps/news/internet-things-helping-provide-key-evidence-criminal-trials
[16] https://ico.org.uk/media/about-the-ico/documents/2617838/ico-report-on-mpe-in-england-and-wales-v1_1.pdf
[17] https://library.college.police.uk/docs/college-of-policing/APP-the-extraction-of-material-from-digital-devices-2021.pdf

read or recover, such as by physically damaging a drive, thus data recovery is not always possible (Battula et al, 2009). Users also take privacy-conscious decisions due to the perceived intrusiveness of smart home devices and, for instance, physically block the view of cameras (Chalhoub et al, 2021). Data can be lost due to accidental events too, such as powering down a smart television (Sutherland, Read & Xynos, 2014).

Reliability of data: Data gathered throughout the digital forensics' procedure requires thorough checks for reliability. For instance, using Global Navigation Satellite System (GNSS) data logs as evidence can face vulnerabilities due to signal blockage, errors, deliberate jamming of the receiver, spoofing of the signal, tampering with the device in case of on-board data storage and falsifying positions when data is stored elsewhere (Dempers, 2018).

Volume of data: The relative decrease in cost of data storage spaces has led to more digital traces to manage and investigate. This creates challenges such as increasing time to sift, analyse and interpret data within investigations (Rogers, 2015). The increase in data volume may impact effective use in investigations due to limitations in technical capabilities to handle IoT traces (Rappert, Wheat & Wilson-Kovacs, 2020). The result-oriented and time-sensitive nature of forensic investigations generates demand for new tools to enhance efficiency, such as automating certain phases (Casey, Katz & Lewthwaite, 2013).

Interpretation of data: The interpretation of digital evidence may require tying activity to the account holder, a common issue in digital forensics. Given IoT in smart homes may be in communal spaces shared by householders, the account holder may not be the (only) user of the device, unlike with a smartphone which is more often personal. So, if an IoT device has the account holder signed in, supporting evidence may be needed to increase certainty that activity links to that account holder (Rogers, 2015). For example, location data from mobile phones can be used to determine whether the device was in the home or not, with rough estimates of

locations based on GSM signals since 1996 (Drane, Macnaughtan & Scott, 1998). But finding the presence of a picture or a GPS coordinate may not be enough to do this and instead, multiple traces need to be examined (Kaart & Laraghy, 2014). Combined with other types of data, such as online browsing activity and biometric data, location data can pinpoint if a particular user of the device was at home. Further, Kim et al (2020) have shown that smart home devices contain data regarding other online activities including phone calls, TV viewing behaviour, use of certain applications alongside recording digital traces of offline actions, such as whether a person was moving around, if they entered or left the home or whether they engaged in a particular activity at the time, for example through data from sensors or voice commands. Such data helps link activity on a shared device to a particular user, creating the necessary link before it can be used to support police investigations.

Tampering with data: As with traditional evidence, it is possible to tamper with and falsify digital evidence too, with a plethora of tools and techniques enabling users to remove digital traces or prevent their creation. These include encryption, secure methods of data deletion, the removal of operating system artefacts, the removal of traces of online activities (Lees, 2013), deleting frames in video recordings (Shanableh, 2013) and faking timestamps (Cho, 2013). It is also possible to fake certain type of biometric data, such as face ID (Cho & Jeong, 2017) or fingerprints for the purposes of unlocking a smart phone (Bontrager et al, 2018; Tait, 2021). Some other technological challenges include maintaining the chain of custody as devices usually '*actively intercommunicate among themselves including the cloud servers*' when they are seized (Janarthanan, Bagheri & Zargari, 2021, pp 232). Solutions might include use of digital forensic readiness frameworks for smart homes to enable evidence gathering e.g. as exist for cases of cybercrime attacks (Philomin et al, 2020).

Narrative Building from Data. In using IoT trace data, novel risks arise for police narrative building. For example, partial data might be 'interrogated' and interpreted to make inferences

that help to confirm a specific hypothesis leading to *confirmation bias* (Innes, 2007; O'Brien, 2009). Traces might help to find a link between an individual and the crime scene resulting in a 'suspect-centred approach' where personal bias and tunnel vision of investigators might skew judgment (Tung and Bowling, 2006). This is particularly problematic if this leads to prioritisation and targeting of wrong individuals (Innes, 2007). IoT data needs to be contextualised to make sense of what human activity is being inferred. This is a shift from traditional forensics, where it goes beyond the presence of a piece of trace evidence (e.g., a fingerprint present at a scene) to help construct a narrative (e.g., the perpetrator was present at this location). Instead, with IoT traces, there is need to construct what the data shows in the first place e.g., high levels of water usage at an unusual time of day on a water meter – is this a leak? Or evidence of a crime scene being washed down?

Legal Implications. Whilst this paper does not focus in depth on the legal issues of IoT digital forensics, there are some key challenges to note. IoT raises cross border policing issues for accessing remote cloud servers for evidence acquisition (Wall, 2017; Walden, 2013). It also highlights reliance on state-industry cooperation e.g., as seen with Amazon or Apple resisting court orders to hand over data[18]. International legislative initiatives are changing the landscape here, for example, with the recently negotiated Second Protocol to the Council of Europe Cybercrime Convention which adds new rules for law enforcement access to cloud data and cross border cooperation. There are growing trends in edge and fog computing to manage latency, privacy and storage issues of current IoT, which means next generation IoT devices are less reliant on the centralised cloud and instead store data (and even perform analytics) locally (Satyanarayanan, 2017). This could change how evidence is acquired, where more data might be on device, than being split in the cloud and device. There are also evidentiary questions around admissibility of IoT data following investigations, and how intrusions by

[18] https://www.bbc.co.uk/news/technology-35601035

police into private and family life by seizing hybrid digital/physical IoT devices might be justified (or not) under police procedure rules e.g. ultimately in line with the Right to Private and Family Life in Art 8 European Court of Human Rights jurisprudence or Fourth Amendment in the USA.

PART 3. Living with Invisible Witnesses.

In this section, we reflect on what it means to live with 'invisible witnesses' in the home, specifically the surveillance implications of making techno-mediated domestic life visible to third parties. There are two elements to this; firstly, considering how IoT is domesticated into the home with differing levels of control for different occupants; secondly the loss of personal space by permanent IoT surveillance, using Goffman's metaphor of both the *frontstage* and *backstage* of everyday life.

We first consider the *degree of choice* home occupants have over bringing IoT devices into the home and how this shapes IoT becoming embedded in their daily lives. It has been long acknowledged that motivations for interacting with surveillance technologies can be playful (Albrechtslund, 2008) or for pleasure (Lyon 2001 and 2017). Some consumers may choose to acquire smart speakers for entertainment or wearable devices for health management voluntarily, bringing surveillance tools like microphones and body sensors into their lives. This can raise issues of trade-offs, where there are both benefits and risks of use e.g., as Makinen (2016) found with smart home security where benefits of safety in the home were balanced against perceived spying on other occupants.

However, sometimes those living in smart homes have not chosen to be subject to these systems and thus face differentiated levels of control over how shared spaces are surveilled. Geeng and Roesner (2019) examined management of smart home devices, observing the

occupant who chooses to install and maintain the device to exert control over use and access to the devices. Zeng et al (2017) echo this point, highlighting concerns about dominance and control through devices monitoring other occupants. Similarly, Goulden (2021) has highlighted the challenges home occupants face around management of IoT accounts and the power asymmetries and control these enable between household members. Freed et al (2018) and Spulska and Tanczer (2021) have explored aspects of how such devices can become tools of intimate partner violence to coerce, monitor, and threaten. This shows the complexity of how users interact with and domesticate IoT systems to different extents in their everyday lives.

As the Covid-19 pandemic has shown, routines change, and 'new normal' practices can emerge. As Bauman and Lyon (2012) have argued, contemporary life is not static, is constantly being remade and is 'liquid' with surveillance and domestic practices similarly changing. Predictions state many companies are planning to shift at least a part of their workforce to permanent home working,[19] increasing the amount of time spent at home and conduct enabling data to be observed across different contexts of life. IoT then, has scope to put professional and private aspects of life under permanent surveillance.

This has consequences, and Rapoport (2012) explores how loss of the home as an 'enclave of privacy and retreat' can occur through the integration of smart technologies. The integration of these technologies into the home reframes boundaries and notions of private space by contrasting it to logics of public space surveillance. Rapoport highlights how assemblages of smart devices can change the nature of experience of domestic, everyday interactions stating "domestic users are not only interpolated as subjects, but also assume heightened agency as they take control over their physical environment and over the projected image of their bodies." (p331). Similarly, Ball (2009) has highlighted the importance of

[19] https://www.forbes.com/sites/carolinecastrillon/2021/12/27/this-is-the-future-of-remote-work-in-2021/

thinking about subjective experiences of surveillance and the ways in which surveillance can enable exposure of the interiority of subjects in different ways. Subjects may purchase these smart home devices for convenience, pleasure, or safety. But the subjective experiences of exposure from smart device surveillance turn on who is in control within the home. For example, if devices are deployed by choice as the operator or if another occupant is subject to being monitored by their cohabitee. There are also impacts of exposure arising from access by third parties (e.g., unanticipated use by police in investigations vs anticipated use by IoT vendors).

Taking this point further, digitisation of the home environment via IoT increasingly means it makes the 'front stage' of everyday life visible, where in the past the home would have been the 'backstage', beyond view. Goffman theorised that in interpersonal interactions people, either deliberately or subconsciously, present themselves in a certain performative way (Goffman, 1956, p3). Individuals or teams may emphasise or conceal particular facts or fragments of their characteristics and personalities in order to '*keep up the impression the performance fosters*' and to keep their secrets (Goffman, 1956, p87). Overall, there are three roles in every performance: *the performers* (who appear in both the front and back regions of the performance), *the audience* (who only appear in the front region) and *the outsiders* (who are excluded from both regions) (Goffman, 1956, p90).

This is a key observation from our perspective as this alters crucially with the emergence of smart home devices that can keep records of different activities that a person or a team does in the backstage of their performances *over time*. This change can be conceptualised in two ways. The previously inaccessible backstage suddenly becomes potentially visible to both the *audience* and the *outsiders*, while still keeping its backstage nature as most users are not aware of the extent of the data collection and usage. As this can occur over long timeframes, with technologies becoming domesticated, this is not a transient but systematic observation of the

backstage and the range of outsiders enabled by smart devices are broad with advertisers, other companies and police.

The Goffman frontstage / backstage metaphor has been used by privacy scholars in the past (Westin, 1968; Koops, 2018). Koops usefully extends the idea to consider the importance of spatial boundaries in life, such as the home, in order to maintain *privacy spaces* i.e., domains '*to play in your own way, the social roles of your life*' (p613) As he states, "*having privacy spaces is an important presupposition for autonomy, self-development, and the other values that privacy contributes to…*" (p621). His conception draws on Goffman explicitly arguing, "*in short, in your own room, you can truly be yourselves, in all senses of being let alone: backstage relaxation from playing social roles, having no fear of observation or judgement of others, and having utmost control over information flows.*" (p634). In the smart home, this division can be harder to maintain, but this quote shows the other values that are contingent on carving out physical spaces for enabling privacy. In a later paper Hoepman and Koops (2020) further consider the importance of protecting domestic space, showing how users can limit law enforcement access to their private files in the cloud through different encryption, hardware, and physical control approaches. This translates to smart devices given the reliance on cloud storage but IoT could raise further challenges, such as differentiated or lacking user interfaces that, unlike with laptops or smartphones, could impact the user's ability to set-up encryption or manage storage effectively (unless another device acts as a mediator). The limited ability of users to choose what storage setup smart device vendors provide out the box is distinct to the web or mobile domain, where there is often greater agency over these choices. Further, the general state of IoT privacy and security has highlighted greater support for users is needed to manage their data management risks (Urquhart & Chen, 2021) e.g., more usable oversight dashboards of what devices are collecting, sharing, and who is accessing this. Future technical defaults and shifts in IoT architectures away from primarily cloud storage towards edge-based

storage and data processing, in conjunction with on device hardware like trusted execution environments, could give users greater local control again over their data storage. This may change how police use smart devices in future investigations and the interplay between seizure of physical smart devices and reliance on obtaining data from the cloud.

PART 4. Final Reflections.

As has been shown, IoT enables sensing of users' daily routines, capturing traces of digital interactions through different sensors and devices embedded in the home. Designed to be invisible in use, these devices can act as 'invisible witnesses'. They also create new forms of domestic and IoT enabled surveillance, building new forms of visibility of everyday life, thus becoming a new class of witness relevant to police forces. This article presented a conceptual analysis of these new forms of (in)visibility in the home and below we briefly summarise the 3 main contributions of this analysis.

Key Point 1. Invisible in Use.

The first key point is that smart devices are embedded in settings where our interactions and everyday life occur (Lyon, 2018). Traces of such interactions are captured and made visible by devices which are designed to be invisible (Tolmie et al, 2002; Weiser, 1994). They are embedded in settings where our interactions and everyday life occur (Lyon, 2018), but they are designed to be unseen. Acting as 'invisible witnesses', they not only capture mundane practices and routines, but also observe and enable control dynamics and power asymmetries in the domestic setting (Crabtree & Rodden, 2004).

Key Point 2. Visibility of everyday life and crime.

The second key point is that ultimately these devices create visibility not only of everyday life practices but also of criminal activity involving home occupants. The Covid-19 lockdown measures changed daily routines at home in many countries and, at least in the UK, altered crime trends and dynamics (e.g., increase in domestic abuse and intimate partner violence).[20] The visibility and metamorphosis of domestic life and criminal activity is accompanied by changing, 'liquid' surveillance practices (Bauman & Lyon, 2012), here illustrated by IoT and the digitisation of the home environment. With more time spent at home, the domestic setting can become the 'frontstage' rather than the 'backstage' of our everyday life (Goffman, 1956), becoming visible to an *audience* and *outsiders* in which IoT devices play a significant role. Further research must consider the value of this type of evidence in criminal investigation and, more generally, the role of ambient interactive systems in policing. We highlighted the impacts on digital forensics, trace evidence and investigation narratives, but further work is needed to understand the long-term implications of making domestic life visible to criminal investigation processes.

Key Point 3. *Multiple devices, partial stories, and inferences*

When a crime is investigated, a narrative is constructed using trace evidence and witness statements. Different IoT devices can be present at the (smart home) crime scene, collecting digital traces and shaping this narrative. These heterogenous devices can provide multiple narratives of what happened in that domestic setting. This multiplicity of narratives and heterogeneity of data is illustrated in some of the use cases presented above.

As we recall, the 'hot tub' murder case in Arkansas was investigated with the use of both smart speakers and smart water meters. But there were other devices available in that home that were also checked by the police (i.e., a "Nest" thermostat, an alarm system with door

[20] https://www.unodc.org/documents/data-and-analysis/covid/Property_Crime_Brief_2020.pdf; https://post.parliament.uk/technology-and-domestic-abuse/

monitoring alarms and motion sensors, weather monitoring systems, remote-activated lighting devices, etc). These different systems are integrated as part of a puzzle that attempts to piece together different stories. As they *see* different parts of our lives, they all tell provide partial insights into the home. Considering how complex the social space of a home can be, it is important to explore further how the *witness statements* provided by these invisible witnesses might not account for that complexity.

Temporality is also important when considering how these traces of digital interactions are collected. IoT devices enable longitudinal observation and inferences about what is deemed usual or unusual behaviour. Again, in relation to the 'hot tub' murder, the smart water meter was useful because it allowed the police to compare the quantity of water used when the murder occurred and compare this to a normal amount of water used at that time of day. If data revealed that 140 gallons of water were used during a couple of hours when the murder occurred, police were also able to see that house occupants never normally used more than 10 gallons of water per hour. This longitudinal observation shapes the narrative, because it allows the police to make an inference: that amount of water was excessive and was used to clean the crime scene. Such forms of longitudinal visibility around everyday life allow inhabitant routines to be constantly interrogated by these witnesses.

This article attempts to bring different perspectives together from criminology, policing, sociology, forensics, and computing to better understand the nature of smart homes and the implications of the use of IoT by police. Further interdisciplinary research will help unpack further social, technical, legal, and ethical challenges posed by the use of these 'invisible witnesses' in criminal investigations.

Acknowledgements

Paper authors Urquhart, Miranda and Podoletz are funded under the UK Economic and Social Research Council project 'Emotional AI in Cities: Cross Cultural Lessons from UK and Japan on Designing for An Ethical Life' (ES/T00696X/10), and Urquhart is also funded under UK Engineering and Physical Sciences Research Council projects 'Defence Against Dark Artefacts' (EP/R03351X/1) and 'UKRI Trustworthy Autonomous Systems Regulation and Governance Node' (EP/V026607/1).

Bibliography

1. Aarts, E. & Marzano, S. (2003) *The New Everyday: views on Ambient Intelligence*. 010 Publishers.
2. Abowd, D., Dey, A.K., Orr, R. & Brotherton, J. (1998) Context-awareness in wearable and ubiquitous computing. *Virtual Reality 3*, 200-211.
3. Akinbi, A. & Berry, T. (2020) Forensic Investigation of Google Assistant. *SN Computer Science, 1*, Article number 272.
4. Albrechtslund, A. (2008) Online social networking as participatory surveillance. *First Monday, 13(3)*.
5. Asghar, M.R., Dán, Gy., Miorandi, D. & Chlamtac, I. (2017) Smart Meter Data Privacy: A Survey. *IEEE Communications Survey & Tutorials, 19(4),* 2820-2835.
6. Ashton, K. (2009) That 'Internet of Things' Thing. *RFID Journal*. Published on 22 June. 2009. Retrieved from http://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf
7. Ball, K. (2009) Exposure: Exploring the Subject of Surveillance. *Information, Communications and Society.* 12(5), 630-657.

8. Bauman, Z. & Lyon, D. (2012) *Liquid Surveillance: A Conversation*. Wiley.

9. Battula, B.P., Rani, B.K., Prasad, R.S. & Sudha, T. (2009) Techniques in Computer Forensics: A Recovery Perspective. *International Journal of Security, 3(2)*, 27-35.

10. Bell, G., & Dourish, P. (2006) *Divining a Digital Future: Mess and Mythology in Ubiquitous Computing*. MIT Press.

11. Bhat, A., Sharma, S., Pranav, K.R. & Monica Rani, H.G. (2017) Home Automation Using Internet of Things. *International Research Journal of Engineering and Technology, 4(7)*, 917-920.

12. Bontrager, P., Roy, A., Togelius, J., Memon, N. & Ross, A. (2018) DeepMasterPrints: Generating MasterPrints for Dictionary Attacks via Latent Variable Evolution. *Proceedings of IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, October 2018.

13. Casey, E., Katz, G. & Lewthwaite, J. (2013) Honing digital forensic processes. *Digital Investigation, 10*, 138-147.

14. Chalhoub, G., Nthala, N., Kraemer, M.J. & Flechais, I. (2021) "It did not give me an option to decline": A Longitudinal Analysis of the Uner Experience of Security and Privacy in Smart Home Products. *CHI'21*.

15. Cho, G.S. (2013) A computer forensic method for detecting timestamp forgery in NTFS. *Computers & Security 2013(34)*, 36-46.

16. Cho, M. & Jeong, Y. (2017) Face recognition performance comparison between fake faces and live faces. *Soft computing, 21(12)*, 3429-3437.

17. Crabtree, A. & Rodden, T. (2004) Domestic Routines and Design for the Home. *Computer Supported Cooperative Work (CSCW), 13*, 191-220.

18. Crabtree, A. Rouncefield, M and Tolmie, P. (2012) *Doing Design Ethnography*. Springer.

19. Christensen, A. T., Olesen, H. & Sørensen, L. (2021) On the Value of the Counterfactual and How the Smart Home Informs It. *Surveillance & Society* 19(2), 241-243.

20. Dempers, A. (2018) Use of GPS Data as Evidence in Court. *International Global Navigation Satellite Systems Association IGNSS Conference 2018*.

21. Drane, C., Macnaughtan, M. & Scott, C. (1998) Positioning GSM Telephones. *IEEE Communicatios Magazine 1998(April)*, 46-59.

22. European Commission / National Science Foundation (2004) *The Disappearing Computer* Vienna, Austria. https://www.ercim.eu/EU-NSF/DC.pdf

23. Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T. & Dell, N. (2018) 'A Stalker's Paradise': How Intomate Partner Abusers Exploit Technology. *CHI'18: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*.

24. Garfinkel, H. (1967) *Studies on Ethnomethodology*. New Jersey, USA: Prentice Hall.

25. Geeng, C. & Roesner, F. (2019) 'Who's In Control?': Interactions In Multi-User Smart Homes. *CHI'19: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. Retrieved from https://www.franziroesner.com/pdf/geeng-smarthomes-chi19.pdf

26. Goffman, E. (1956) *The Presentation of Everyday Life*. Harmondsworth: Penguin

27. Goulden, M. (2021) 'Delete the Family': Platform Families and the Colonisation of the Smart Home. *Information, Communication & Society, 24(7)*, 903-920.

28. Hoepman, J.H. & Koops, B.J. (2020) Offering 'Home' Protection to Private Digital Storage Spaces. *SCRIPTed, 17(2)*. Retrieved from https://script-ed.org/article/offering-home-protection-to-private-digital-storage-spaces/

29. House of Lords (2019) *Forensic Science and the criminal justice system: a blueprint for change*. HL Paper 333.

30. Innes, M. (2007) Investigation Order and Major Crime Inquiries in Newburn, T. and Williamson, T. and Wright, A. (Eds) Handbook of Criminal Investigation (New York: Routledge) 255-276

31. Janarthanan, T., Bagheri & M., Zargari, S. (2021) IoT Forensics: An Overview of the Current Issues and Challenges. In Montasari, R., Jahankhani, H., Hill, R. & Parkinson, S. (Eds.) *Digital Forensic Investigation of Internet of Things (IoT) Devices* (pp. 223-254). Springer.

32. Kaart, M. & Laraghy, S. (2014) Android forensics: Interpretation of timestamps. *Digital Investigation (2014)11*, 234-248.

33. Kim, S., Park, M., Lee, S. & Kim, J. (2020) Smart Home Forensics – Data Analysis of IoT Devices. *Electronics, 2020(9)*, 1215. Retrieved from https://www.mdpi.com/2079-9292/9/8/1215

34. Kirk, P (1974) *Crime Investigation: Physical evidence and the Police laboratory*. (New York: Interscience Publishers, Inc., 1974. 2nd Ed.)

35. Koops, B.J. (2018) Privacy Spaces. *West Virginia Law Review, 121(2)*. Retrieved from https://researchrepository.wvu.edu/wvlr/vol121/iss2/8/

36. Locard, E (1928) Dust and Its Analysis. *Police Journal* 1(2). p177-192

37. Lees, C. (2013) determining removal of forensic artefacts using the USN change journal. *Digital Investigation (2013)10*, 300-310.

38. Lyon, D. (2001) *Surveillance Society: Monitoring Everyday Life*. Buckingham, USA: Open University Press.

39. Lyon, D. (2017) Surveillance culture: engagement, exposure and ethics in digital modernity. *International Journal of Communication 11*, 824-842.

40. Lyon, D. (2018) The culture of surveillance. Cambridge: Polity Press.

41. Makinen, L.A. (2016) Surveillance on/off: Examining home surveillance systems from the user's perspective. *Surveillance & Society 14(1)*.

42. Malkin, N., Bernd, J., Johnson, M. & Egelman, S. (2018) 'What Can't Data Be Used For?' Privacy Expectations about Smart TVs in the U.S. *European Workshop on Usable Security (EuroUSEC) 2018*.

43. Muir, R. & Walcott, S. (2021) *Unleashing the Values of Digital Forensics*. The Police Foundation. Retrieved from https://www.police-foundation.org.uk/2017/wp-content/uploads/2010/10/value_of_digital_forensics.pdf

44. O'Brien, B. (2009). Prime suspect: An examination of factors that aggravate and counteract confirmation bias in criminal investigations. *Psychology, Public Policy, and Law, 15*(4), 315–334

45. Pridmore, J., Zimmer, M., Vitak, J., Mols, A., Trottier, D., Kumar, P. C., & Liao, Y. (2019) Intelligent Personal Assistants and the Intercultural Negotiations of Dataveillance in Platformed Households. Surveillance & Society17(1/2): 125-131. https://ojs.library.queensu.ca/index.php/surveillance-and-society/index

46. Philomin, S., Singh, A., Ikuesan, A. & Venter, H. (2020) Digital Forensic Readiness Framework for Smart Homes. *Proceedings of the International Conference on Cyber Warfare and Security*, 667-638.

47. Rappert, B., Wheat, H. & Wilson-Kovacs, D. (2020) Rationing bytes: managing demand for digital forensic examinations. *Policing and Society 31(1).*

48. Rapoport, M. (2012) The Home Under Surveillance: A Tripartite Assemblage. Surveillance & Society10(3/4): 320-333. http://www.surveillance-and-society.org

49. Reedy, P. (2021) *Strategic Leadership in Digital Evidence*. London, UK: Academic Press

50. Rogers, M.K. (2015) Psychological profiling as an investigative tool for digital forensics. In Sammons, J. (Ed.) *Digital Forensics: Threatscape and best practices* (pp. 45-58). Elsevier Science and Technology Books.

51. Sacks, H. (1992) *Lectures on Conversation*. Cambridge: Blackwell.

52. Satyanarayanan, M. (2001) Pervasive Computing: Vision and Challenges. *IEEE Personal Communications*. Retrieved from https://www.cs.cmu.edu/~aura/docdir/pcs01.pdf

53. Satyanarayanan, M. (2017) The Emergence of Edge Computing. *Computer, 50(1).*

54. Shanableh, T. (2013) Detection of frame deletion for digital video forensics. *Digital Investigation (2013)10*, 350-360.

55. Silverstone, R., Morley, D., Dahlberg, A. & Livingstone, S. (1989) *Families, technologies and consumption: the household and information and communication technologies*. CRICT discussion paper. Uxbridge, UK: Centre for Research into Innovation, Culture & Technology.

56. Sorensen, K.H. (1994) *Technology in use: Two essays on the domestication of artefacts*. Trondheim, Norway: Centre for technology and society working paper 2/94.

57. Spluska, J., & Tanczer, L. (2021). **Threat Modeling Intimate Partner Violence: Tech Abuse as a Cybersecurity Challenge in the Internet of Things**. In J. Bailey, A. Flynn, N. Henry (Eds.), *The Emerald International Handbook of Technology Facilitated Violence and Abuse*. Emerald Publishing Limited. doi:10.1108/978-1-83982-848-520211049

58. Sunde, N. & Dror, I.E. (2021) A Hierarchy of Expert Performance (HEP) applied to Digital Forensics: Reliability and Biasability in Digital Forensic Decision Making. *Forensic Science International Digital Investigation, 37(2)*. Retrieved from https://www.sciencedirect.com/science/article/pii/S2666281721000834?via%3Dihub

59. Suchman, L. (1987) *Plans and Situated Actions*. Cambridge: Cambridge University Press.

60. Sutherland, I., Read, H. & Xynos, K. (2014) Forensic analysis of smart TV: A current issue and call to arms. *Digital Investigation 2014(11)*, 175-178.

61. Tait, B.L. (2021) Aspects of Biometric Security in Internet of Things Devices. In Montasari, R., Jahankhani, H., Hill, R., Parkinson, S. (Eds.) *Digital Forensic Investigation of Internet of Things (IoT) Devices* (pp. 169-186). Springer.

62. Tolmie, P., Pycock, J., Diggins, T., Maclean A. & Karsenty, A. (2002) Unremarkable computing. *CHI'02: Proceedings of the SIGCHI Conference on Human Factors in Computing*, 399-406

63. S. Tung and B. Bowling, (2006) 'Art, Craft and Science of Detective Work', The Police Journal: Theory, Practice and Principles. 79(4). 323-330.

64. Urquhart, L. & Chen, J. (2021) On the Principle of Accountability: Challenges for Smart Homes & Cybersecurity. Crabtree, A., Mortier, R. & Haddadi, H. (Eds.) *Privacy by Design for the Internet of Things: Building Accountability and Security*. IET Press.

65. Urquhart, L. Lodge, T. and Crabtree. A Demonstrably Doing Accountability in the Internet of Things. *International Journal of Law and Information Technology*, Volume 27, Issue 1, Spring 2019, Pages 1–27, https://doi.org/10.1093/ijlit/eay015

66. Walden, I. (2013) Law Enforcement Access to Data in Clouds. In Millard, C. (2013) *Cloud Computing Law*. Oxford Scholarship Online.

67. Wall, D.S. (2017) Towards a Conceptualisation of Cloud (Cyber) Crime. *International Conference on Human Aspects of Information Security, Privacy and Trust*, 529-538.

68. Weiser, M. (1990) *The Computer for the 21st Century*. Retrieved from https://www.ics.uci.edu/~corps/phaseii/Weiser-Computer21stCentury-SciAm.pdf

69. Weiser, M. (1994) The world is not a desktop. *ACM Interactions, January 1994*, 7-8.

70. Weiser, M. & Seely Brown, J. (1996) *The Coming Age of Calm Technology*. Retrieved from https://boccignone.di.unimi.it/IUM2_2013_files/weiser-calm.pdf

71. Westin, A.F. (1968) Privacy and Freedom. *Washington and Lee Law Review, 25(1)*. Retrieved from https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20

72. Wilson-Kovacs, D (2020) Effective resource management in digital forensics: An exploratory analysis of triage practices in four English constabularies. *Policing: An International Journal, 43(1)*, Published online: 6 April 2019.

73. Wilson-Kovacs, D., Rappert, B. & Redfern, L. (2021) Dirty Work? Policing Online Indecency in Digital Forensics. *The British Journal of Criminology*. Published online: 21 June 2021. Retrieved from https://doi.org/10.1093/bjc/azab055

74. Yang, R. & Newman, M.W. (2013) Learning from a learning thermostat: lessons for intelligent systems for the home. *UbiComp'13: Proceedings of the 2013 ACM International Joint Conference on Pervasive and ubiquitous computing*, 93-102.

75. Yang, S.J., Choi, J.H., Kim, K.B., Bhatia, R., Saltaformaggio, B. & Xu, D. (2017) Live acquisition of main memory data from Android smartphones and smartwatches. *Digital Investigation, 23*, 50-62.

76. Zeng, E., Mare, S. & Roesner, F. (2017) End User Security and Privacy Concerns with Smart Homes. *SOUPS 2017: Proceedings of the Thirteenth Symposium on Usable Privacy and Security*. Retrieved from https://www.usenix.org/system/files/conference/soups2017/soups2017-zeng.pdf

77. Zatyko, K. & Bay, J. (2014) *The Digital Forensics Cyber Exchange Principle*. Originally published on DFI News (www.dfinews.com). Retrieved from http://www.csc.villanova.edu/~dprice/fall2014/extra_handouts/The_Digital_Forensics_Cyber_Exchange_Principle_-_2013-04-22.pdf