



Kent Academic Repository

Shere, Anjuli R.K., Nurse, Jason R. C. and Martin, Andrew (2023) *Threats to Journalists from the Consumer Internet of Things*. In: *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media. Cyber Science 2022*; 20–21 June; Wales. Springer Proceedings in Complexity . Springer ISBN 978-981-1964-13-8.

Downloaded from

<https://kar.kent.ac.uk/94898/> The University of Kent's Academic Repository KAR

The version of record is available from

https://doi.org/10.1007/978-981-19-6414-5_17

This document version

Author's Accepted Manuscript

DOI for this version

Licence for this version

UNSPECIFIED

Additional information

Versions of research works

Versions of Record

If this version is the version of record, it is the same as the published version available on the publisher's web site. Cite as the published version.

Author Accepted Manuscripts

If this document is identified as the Author Accepted Manuscript it is the version after peer review but before type setting, copy editing or publisher branding. Cite as Surname, Initial. (Year) 'Title of article'. To be published in **Title of Journal** , Volume and issue numbers [peer-reviewed accepted version]. Available at: DOI or URL (Accessed: date).

Enquiries

If you have questions about this document contact ResearchSupport@kent.ac.uk. Please include the URL of the record in KAR. If you believe that your, or a third party's rights have been compromised through this document please see our [Take Down policy](https://www.kent.ac.uk/guides/kar-the-kent-academic-repository#policies) (available from <https://www.kent.ac.uk/guides/kar-the-kent-academic-repository#policies>).

Threats to Journalists from the Consumer Internet of Things*

Anjuli R.K. Shere¹, Jason R.C. Nurse² and Andrew Martin³

¹ Department of Computer Science, University of Oxford, Oxford, United Kingdom
anjuli.shere@cs.ox.ac.uk

² School of Computing, University of Kent, Canterbury, United Kingdom
j.r.c.nurse@kent.ac.uk

³ Department of Computer Science, University of Oxford, Oxford, United Kingdom
andrew.martin@cs.ox.ac.uk

Abstract. Threats associated with the consumer Internet of Things (IoT) may particularly inhibit the work and wellbeing of journalists, especially because of the danger of technological surveillance and the imperative to protect confidential sources. These issues may have knock-on effects on societal stability and democratic processes if press freedom is eroded. Still, journalists remain unaware of potential IoT threats, and so are unable to incorporate them into risk assessments or to advise their sources. This shows a clear gap in the literature, requiring immediate attention. This article therefore identifies and organises distinctive and novel threats to journalism from the consumer IoT. The article presents a novel conceptualisation of threats to the press in six categories: regulatory gaps, legal threats, profiling threats, tracking threats, data and device modification threats, and networked devices threats. Each of the threats in these categories includes a description and hypothetical consequences that include real-life ways in which IoT devices can be used to inhibit journalistic work, building on interdisciplinary literature analysis and expert interviews. In so doing, this article synthesises technical information about IoT device capabilities with human security and privacy requirements tailored to a specific at-risk population: journalists. It is therefore important for cyber science scholarship to address the contemporary and emerging risks associated with IoT devices to vulnerable groups such as journalists. This exploratory conceptualisation enables the evidence-based conceptual evolution of understandings of cyber security risks to journalists.

Keywords: Internet of Things, Smart devices, Journalism, Threats, Security, Privacy, Risk assessments.

* Article to be published in *Proceedings of the 2022 International Conference on Cybersecurity, Situational Awareness and Social Media (Cyber Science 2022)*

1 Introduction

Often touted in the media as the next great technological trend, the consumer Internet of Things (IoT) market has seen rapid growth in recent years, with devices becoming increasingly prevalent in public spaces, private places and even on bodies [1]. The general security ramifications of this expansion have been widely discussed (e.g. [2–4]); however, there are few user-specific assessments of privacy and security threats that can be enacted using IoT devices, and none relating to journalists. Our pilot study involved interviewing and surveying members of the media from around the world to establish the extent to which they interact with the IoT and their knowledge of associated threats [5]. This study determined that this community is particularly vulnerable to IoT threats because of a lack of understanding of how these new technologies could increase risk to the work and wellbeing of members of the press and their sources, and of what can be done to mitigate these threats [5]. Further, journalists merit being the focus of research into IoT threats because of the public-facing nature of their job, which increases their risk level [6–10], and also means that any consequences of successful attacks may extend far beyond an individual journalist and potentially destabilise other democratic infrastructure [11–13].

Educating the press about such threats is crucial because the IoT is inherently and systemically insecure, demonstrated by a survey that showed both that “almost 70% of all IoT devices to be prone to privacy threats” and “every IoT device is responsible for at least one piece of personal information collection” [14]. Extensive risk assessments are of particular importance to the media industry, as state-affiliated cyber attackers are increasingly targeting journalists [15]. As journalists are already highly targeted, any interaction that they may have with the consumer IoT creates a concerning expansion of their attack surface. Comprehensive risk assessments cannot be carried out without accurate threat modelling that facilitates prioritisation of security strategies and techniques.

As the IoT is an evolving and growing phenomenon, it is impossible to identify all associated risks and the threats from which they arise. Therefore, this article uses existing literature to propose a novel conceptualisation that explores ways in which these threats can manifest against the press, largely relating to surveillance [16]. Journalists’ understanding of their cyber security [17–19], and how IoT devices could present a threat remains low [5]. These new IoT threat categories explore impacts and implications of IoT devices for the media, to increase understanding of the societal effects of surveillance and kinetic threats to journalists from these technologies.

2 Related work

The literature in this section influenced the structure of the categorisation. The most relevant sources that were used for the taxonomy’s content have been cited in Section 4.

2.1 IoT and journalism threat modelling

Like Uzunov and Fernandez [20], our paper views threat modelling as useful for demonstrating the interlinked nature of different threats from the same system, and as a conceptual foundation for systematically organising emerging threats within an existing framework [21–23]. Xiong and Lagerström [24] discuss that articles in this area either introduce a new method, use an existing threat modelling approach, or present work on the threat modelling process; our article aims to do the first and third of these, i.e. to explore an IoT-related threat model that is specific to and can be used by members of the media. Our threat modelling relies on the creation of scenarios, similar to other informal threat modelling systems for conventional cyber threats to journalists [25–27]. However, although such materials may touch upon physical and legal threats, these are beyond their scope. Further, none of them consider the expanded threat landscape resulting from the increasing prevalence of the IoT.

The Rory Peck Trust has an online risk assessment that journalists can use before they go on an assignment, but it does not mention IoT devices [28]. McGregor et al.'s study assessing the cyber security behaviours and needs of journalists also did not include the IoT [17]. However, the human-computer interaction and cyber security literature relating to IoT threat modelling spans academic, policy and commercial materials. Each sphere has produced taxonomies or risk assessment considerations with different classifications, according to the needs of their target audience. Our paper explicitly focuses on the press as our target population, in order to cater to their specific needs.

McGregor and Watkins found that journalists relied on a mental model of information security that allowed them to operate with minimal consideration for security precautions (deemed 'security by obscurity'), "unless one is involved in work that is sensitive enough to attract the attention of government actors" [19]. Even an article discussing the implications of "tech tools" used by a technology and media journalist did not mention IoT devices at all, but instead solely focused on smartphone applications and the consequences of targeted advertising [29]. Similarly, our pilot study found that news organisations' cyber protection policies and strategies currently do not incorporate the IoT [5]. Based on this, our categories and threat titles are followed by hypotheticals that describe possible consequences of such threats for the press.

While Gulzar and Abbas's taxonomic structure linked aspects of the IoT with vulnerabilities and threats [14], it does not address the practical consequences of these threats. Nawir et al.'s taxonomy of attacks on IoT security is largely categorised by attack vector [30]; however, some of the attacks in the taxonomy are described in terms of consequences, rather than technique (e.g. "Denial of Service attacks"). This is similar to a home-based IoT security evaluation by Alrawi et al. [31]. Our article therefore builds on both of these taxonomies to make them directly applicable and relevant to a specific user population, and incorporates them especially into the networked devices threats category.

2.2 IoT privacy threats

There are debates on the effects of the consumer IoT on users' and bystanders' privacy, as well as the potential for the IoT to include privacy-enhancing technologies.

Perez et al.'s research addressed an important phenomenon: solutions for IoT-related threats to bystanders' privacy [32]. Similar to Lopez et al. [33], Perez et al.'s paper focused specifically on privacy but overlooked the associated secondary effects of additional security implications that our article discusses. Goulden et al. also noted that pervasive monitoring by these technologies forces the ongoing renegotiation of interpersonal relationships because inhabitants cannot avoid their data being collected and shared in a communal smart home [34].

Christensen et al. acknowledged the dangers of pattern of life recognition and the problems associated with devices' essential functions being reliant on opting into surveillance features [35], which means that many such devices are unusable for journalists with something to hide; this is particularly relevant to our legal threats category. Burdon and Cohen argued that smart homes result in modulation harms and therefore social shaping [36]; this is particularly concerning for journalists, who have societal influence. Our paper draws on this literature, specifically relating to the profiling and tracking categories.

Cha et al. grouped privacy-enhancing technologies into seven categories of protection mechanisms against IoT-related threats to privacy [37]. However, while the privacy issues covered are extensive, the paper did not discuss the risks and needs associated with different user communities. This is the gap our article fills, focusing on a sector that has been limited in its ability to expose the dangers of such data collection [38].

2.3 IoT material threats

An IoT-specific element of threat modelling relates to material threats. Additionally, the use of scenarios by Tanczer et al. influenced the presentation of our paper's descriptions of hypothetical consequences for journalists [3]. Heartfield et al. [39] and Blythe and Johnson [40] instead viewed these threats through the lens of external adversaries. Similar to Tanczer et al., Blythe and Johnson's systematic review of consumer IoT-related crimes extrapolated from existing capabilities and evidence of the facilitation of malicious activities [40]. We used this perspective to inform our data and device modification and networked devices threat categories. Blythe and Johnson took a high-level criminological approach that seems accessible to lay readers; however, their review did not reference non-academic literature. This may mean that scenarios that are salient to specific practitioner-groups were overlooked.

Lopez-Neira et al. cited reports from charities such as Refuge as evidence that cyber-physical attacks are already occurring, to demonstrate the feasibility of the misuse of IoT technologies to facilitate abuse targeting individuals [41]. They noted the difficulties associated with the prevalence of IoT devices, but did not attempt to survey or categorise IoT threats to individuals.

Broadly, studies such as Chalhoub et al. [42] and Barbosa et al. [1] established how user experience and attitudes influence the poor security by design of the consumer IoT. Further, like Hoffmann's policy proposal document on smart home policy [43], Atamli and Martin [44] provided recommendations for long-term changes such as IoT security and privacy properties by design that would address some of their identified threat model characteristics. The threat categories presented in our paper could educate journalists about IoT threats until the IoT industry implements such principles; these issues specifically are addressed by our regulatory gaps threat category.

3 Methods

3.1 Research questions

Two research questions were developed from previous research on this topic, which demonstrated that journalists are not cognisant of consumer IoT threats and do not currently have access to relevant educational resources [5]. These questions are: (1) "What are the distinctive and novel threats to journalism from the consumer IoT?" and (2) "How can we categorise these threats in a way that is easily comprehensible by journalists?"

3.2 Literature synthesis

Curating both related work (Section 2) and the taxonomy (Section 4) drew inspiration from the Preferred Reporting Items for Systematic Reviews and Meta-Analyses guidelines [45]. Sources included academic publications (e.g. in the fields of Journalism Studies, Law, Computer Science and Cyber Security), news articles, websites aimed at journalists, and policy papers, to ensure that this research reviewed all germane perspectives.

Using the research questions to guide our information-gathering method enabled us to find the most contemporary and salient publications available relating to consumer IoT threats to the press. At first, the review began by using assorted combinations of search terms from the research questions and these topics more broadly, such as "consumer Internet of Things", "IoT", "smart home", "security", "privacy", "threat model" and "journalism". Keywords later included other frequently recurring terms in our results, such as "journalist safety", "surveillance", "source confidentiality" and "legal threats".

3.3 Analysis

The findings of the literature search were classified through thematic coding and analysis using NVivo. Categories and their contents were then updated through secondary source analysis of existing IoT threat taxonomies. Codes from literature were sorted into six categories: Legal, Media (codes for information regarding journalists as a minority population under threat), Vulnerabilities, Targets, Attacks, and Impacts.

While there is no hierarchy to the codes or their categories, the latter four categories were ordered to emulate the chronological threat process. Plurals and noun/verb variations of the same code were considered to be the same code (e.g. device/devices, access/accessing), codebook available upon request.

3.4 Category creation

This paper represents an initial exploratory step toward categorising and conceptualising threats in the context of a specific target population, rather than an exhaustive list of potential IoT threats to journalists. Our article categorises nineteen IoT-specific threats that have the potential to harm journalists' work and wellbeing into six categories. Our goal is not a complete or definitive threat taxonomy, but rather to present six clear and relevant categories of threats: (1) regulatory gaps, (2) legal threats, (3) profiling threats, (4) tracking threats, (5) data and device modification threats, and (6) networked devices threats.

As discussed in Section 2, these categories were created by compiling information on potential vulnerabilities and associated exploitation opportunities from academic studies into IoT threats and news sources discussing cyber-attacks on the press. The key inclusion criterion was that current feasibility of the threats must have been evidenced in academic and news materials. The categories were subsequently refined using thematic analysis and by eliminating any threats that were insufficiently relevant to the consumer IoT, then by grouping the remaining nineteen threats into overarching categories.

Each category has its own description, titles and descriptions of some associated threats, and example consequences to illustrate how they would specifically harm press freedom. This last element is presented as a threat scenario that affects journalists, news organisations and the press more generally. Our chosen structure of method of categorisation is informed by the utility of communicating consequences as scenarios to a narrative driven audience such as the media [46], despite the difficulty of finding evidenced examples because IoT threats can be clandestine [47].

3.5 Threat modelling

There are already established methods for threat modelling in cyber security, such as the MITRE ATT&CK framework [48] and STRIDE, the latter which was used by Hoffman for her IoT threat modelling [43]. Like STRIDE, the method of categorization that we outline in this paper is not designed to be as exhaustive as a taxonomy; rather, our categorisation is intended to be an interactive aid for journalist security training, built upon as members of the media engage with this threat modelling exercise, so that more subcategories and hypothetical consequences can be added over time. However, journalists generally process information in more linear and narrative forms, making technically-focused methods less helpful for explaining the ways in which IoT threats could manifest specifically against journalists.

Our paper considers the term threat modelling to refer to curating accurate information on specific threats, which can then be used to create systemic risk

assessments with clear prioritisation at news organisations. Delineation of the clusters of threats was iterative, to capture emergent threats and predictively include them in the mapping process. The goal was to design the categories to be sustainable, robust, and able to include future technologies.

4 Categorisation

Our six categories of threat involve varying degrees of risk, with the severity of different threats depending on the individual circumstances and work of each journalist, their colleagues and their sources.

All six categories are technically possible and ranking them in order of likelihood of occurrence is difficult because the IoT is currently rapidly growing and expanding in scope, and likely threat actors against journalists (e.g. nation-states and organised criminal groups) are not hindered by the cost associated with prolonged or layered attacks. Some of these threats are less likely than those that simply require the journalist to have a phone, as there are well-established threats to journalists that have similar consequences, such as spyware [49–51]. However, for journalists who are engaging with the security advice that is media-focused and relates to traditional technologies, the IoT may be an overlooked area of risk. For example, journalists may be aware of overzealous data collection by IoT devices such as voice assistants, but may not recognise the possibility of use of the voice recordings to activate other devices' functionalities without their knowledge (see category 6).

These categories, described in detail in this section, are: (1) regulatory gaps, (2) legal threats, (3) profiling threats, (4) tracking threats, (5) data and device modification threats, and (6) networked devices threats. There is academic and news coverage of such threats relating to categories 1, 2, 3, 4, and 6. The threats in categories 5 and 6 are characteristic of IoT capabilities that other consumer technologies largely do not share. Of these two categories, 5 (data and device modification threats) is an outlier as it has less overt and more psychological implications, so it is hard to find evidence that it has been enacted in practice; whereas 6 (networked devices threats) has been amply demonstrated by journalists, state agencies and researchers [52].

Due to the commodification of data as integral to the technology industry, a theme underpinning all categories and their contents is that information collection – and, in some cases, leakage – is an intentional feature of IoT technologies, rather than a bug [53–56]. As a result, threats can occur in tandem; for example, a fitness tracker dataset of millions of users may allow easy isolation of a specific journalist's account data (category 4), which would potentially identify their home address and the locations where they meet sources if usernames are cross-referenced with information found on the public-facing social media page of a high-profile journalist (category 3). This could lead to threats to the journalist's specific device (categories 5 and 6). The complexity of multiple steps, as detailed in this example, may make such an attack less likely than a single example from one category, but the compounding potential of these threats is an important feature of networks such as the IoT.

See Sections 3.3 and 3.4 for information on how the categories were created.

4.1 Regulatory gaps

Poor inbuilt IoT security results from lax legal restrictions regarding security and privacy by design. Data is left vulnerable because, e.g. security settings are configured to an inadequately low default, and it is unclear how users can alter them [57]. A feature of this is that apps and the IoT devices on which they are hosted often have weak authorisation protocols that allow overreach, including downloading malware, which could facilitate data theft and manipulation via third party software or device layers, either in storage or in transit [58]. The resultant ambiguity as to whether a journalist is responsible for specific information, either through sharing or creation, could have ramifications for their credibility and public trust.

Third party supply chain actors accessing data. For reasons such as maintenance, IoT device manufacturers can legally ensure that devices continually upload data to, e.g., peer-to-peer networks that are coordinated by the manufacturer, regardless of the length of the chain of components and actors within these networks [59]. Data collected by consumer devices is therefore made accessible to an indeterminate number of parties, regardless of the knowledge or active consent of device owners [60].

Hypothetical consequences. This supply chain risk means that journalists could have their technology and data compromised because they – necessarily or inadvertently – agreed to information sharing with third party actors in this chain.

Data manipulation as a result of consent requirements. Some apps and IoT devices require users to consent to all manner of data acquisition, transfer and processing, as well as allowing access to other device functionalities (such as cameras, microphones and messaging systems) in order to function [57]. Similarly, with the evolution of deep fake technologies, the wealth of data created by IoT devices could be used to effectively and potentially legally use an individual’s likeness.

Hypothetical consequences. These consent requirements allow the problematic potential for access and manipulation of journalists’ data, possibly in ways that could dupe or reveal sources [57].

Data harvesting from decommissioned devices. A situation in which adversarial physical access to devices would be problematic relates to individual journalists or news organisations disposing of defunct or decommissioned IoT devices without appropriately wiping them of their history. This could enable “dumpster divers” to fish out devices and recover confidential information stored either in the device’s local memory or in the cloud, through the device. For many devices, there is no obvious reset button, and the physical device may be an easy entry-point to the user data still retained by the device’s managing company [61].

Hypothetical consequences. Adversaries viewing information on Internet of Things devices could leave journalists and news organisations exposed to data theft relating to finances, employees, security, etc. (i.e. anything that has been accessed via some

devices, and anything mentioned in front of other devices), which could be devastating for both the newsroom and the organisation as a business.

Botnet creation. There is currently no legal or financial incentive for manufacturers to encrypt data or otherwise increase the security of purchased devices; this leaves endpoint management unsupported as devices have out of date firmware or software that can be exploited through well-known channels [43]. As a result, IoT devices, while potentially low-powered on their own, generally have such lax security that they can be easily co-opted into botnets, i.e. networks of (even unrelated and disparate) IoT devices that have been infected with malware.

Hypothetical consequences. Host takeover resulting in botnets can execute data breaches, Distributed Denial of Service (DDoS) attacks on well-secured networks or internet infrastructure [62], and further malware delivery that can drastically affect services on which society relies, including news provision [59, 63, 64]. Any of these activities can be devastating for individual journalists and for news organisations, both of which might be at risk of losing access to vital devices or systems for indeterminate periods of time, as well as the potential that data held on those systems has been compromised [65]. Further, botnets could be used to launch large-scale online attacks on members of the press using troll armies [14, 66].

4.2 Legal threats

Legal threats refer to ways in which IoT data or actions might be used either in law enforcement investigations, or to embroil journalists in lawsuits [67].

Abuse of data and privacy laws. There are a number of methods through which Internet of Things data can be accessed by governments, corporations, or even individuals, who know how to exploit ambiguous legal provisions. Journalistic data can therefore be too-easily accessed by third parties via these legal threats. These threats are due to technologically-neutral protections that do not sufficiently differentiate between types of data and devices, and negligent protections in data protection and privacy laws and regulations, all compounded by a requirement that certain kinds of data are retained for lengthy periods of time.

Hypothetical consequences. Data retention laws may be vague on whether they consider clearly identifiable data from IoT devices to constitute metadata, which further risks information because metadata is often allowed to be kept by governments for longer than other kinds of data. For example, Australian metadata retention laws require metadata storage for a minimum of two years. There is already evidence that these laws have chilled the Australian press, as well as counteracting some of the protections of pre-existing source shield laws [68]. Additionally, data protection laws intended to protect individuals' personal data from unwarranted collection or access and exploitation by third parties usually include provisions for their negation for legitimate interest [69], which governments and associated corporations use to justify their access to and use of data and metadata, including from the IoT [70]. Furthermore, the subject

access ("Right to Access") requests enshrined in privacy laws and regulations, such as the GDPR, can also be ambiguous, leaving the data vulnerable to social engineering attempts that enable adversaries to impersonate journalists to access their information [71].

Weaponisation of financial penalties. Criminal actors could exploit news organisations' notable lack of effective security protocols and the potential for IoT devices that are connected to a central Wi-Fi network. They may distribute ransomware that locks journalists and other media staff out of their work, thereby hindering the progress of a story and creating more financial and legal stressors for executives [58]. The financial repercussions of data breaches, on top of the ransom, are significant threats to the normal operation of media organisations and journalists [72, 73].

Hypothetical consequences. A media-industry-wide culture of under-prioritisation of security (often due to lack of funds) increases the likelihood of security breaches, especially from poorly secured IoT devices. This would likely trigger devastating financial pressures [71], including regulatory fines, investigation costs and compensation payments that would force the news organisation to lay off some of its staff [66].

Warrantless bulk data purchase. Government agencies and private companies can legally sidestep journalistic warrant requirements by purchasing bulk user data from service providers, including those that are involved in the maintenance of IoT devices [58, 74, 75].

Hypothetical consequences. Even if a user can purge the logs held on an old device after years of ownership, they may never know how many times that data was transmitted, accessed, consolidated or sold prior to the purge. Historical datasets are lucrative and there are already academic proposals for ways in which service providers can sell IoT datasets to advertisers and other third parties [76]. This creates a rich dataset from which adversaries may isolate key dates and events, in order to cross-reference these with information gathered on suspected journalistic sources, thereby definitively identifying a confidential source.

4.3 Profiling threats

The timing of interaction with automated household and utility devices could allow "pattern of life" information (i.e. detailed daily routines) to be surmised and exploited [36, 37]. In addition to the potential for behavioural manipulation via IoT "nudging" [77], predictive analysis can also be used to infer more sensitive data by devices or attackers with analytical capabilities, such as one's health status being recognised based on requests made to voice assistants [78], or wearable devices [14, 37, 79]. The IoT-sourced data allows extrapolation to substantiate both true and false scenarios, which could also call into question journalists' professional integrity.

Continuous surveillance. Access level attacks on IoT systems target system availability and can be passive or active, including monitoring and eavesdropping [14, 30]. This ongoing access to information presents the dual issues of both identification of individuals and profiling, i.e. compiling and analysing data on the journalist and their identified sources [14, 37, 80].

Hypothetical consequences. There is the possibility of devices with microphones picking up the sounds of nearby typing patterns, to allow reconstruction of messages sent, which could compromise confidential communications between journalists and their sources and editors, even when sent through secure channels [81]. Access to the huge amounts of personal information gathered by IoT devices, either historic data (such as location information from a fitness tracker [79], or live data such as hacking the camera of a smart television, which may record both video and audio [82]) can facilitate the doxxing and stalking of journalists. In addition to the physical security, health and safety consequences of doxxing and stalking, they could also result in financial and reputational damages that harm journalist's credibility [58].

Abusing health and biometric information. Journalists' portable or wearable devices to track personal health information may not have the inbuilt security to prevent leaks. Malicious actors may use this information to cause psychological or physical distress, thereby influencing a journalist's output, e.g. through blackmail [30, 37].

Hypothetical consequences. Insecurity of wearable fitness or medical devices, including those that collect health information can contribute to inaccurate diagnoses and prescriptions, or even altered test results. These flaws could be fatal and could be used to put psychological, financial or physical pressure on journalists [30, 37]. A feasible but unlikely example is a diabetic journalist having a wearable blood sugar tracker that can be hacked, enabling adversaries to identify vulnerable moments [37, 66].

Data linkage and aggregation. The heterogeneity of IoT devices and their capabilities means that data linkage and data aggregation can reveal far more than was previously possible. Insufficient network segregation in smart home systems comprised of varied consumer IoT devices can enable profiling of both users and those with whom they interact.

Hypothetical consequences. This could jeopardise source confidentiality if data and metadata from both ambient and wearable IoT devices is cross-referenced [82]. Further, this can cause identity theft and financial damage [58], which could affect journalists by embroiling them in complex legal cases that leave little time available for them to focus on work and tie up resources.

4.4 Tracking threats

A likely category of IoT threats is the use of devices' data collection capabilities for tracking purposes, generating either contemporary or retroactive movement patterns sold to private companies and government agencies [74]. Tracking journalists and

sources poses a threat to confidentiality that could ultimately chill the press. Knowledge of their pattern of life may also facilitate physical attacks.

Informal additions to state surveillance networks. Consumer IoT networks can become informal features of smart cities, particularly when easily accessible by law enforcement and intelligence agencies. Many Internet of Things camera-equipped doorbells have built-in police access, effectively making them an extension of state surveillance networks [83].

Hypothetical consequences. This centralisation of data could easily facilitate the tracking of journalists by governments without transparent oversight.

SOCMINT and IoT interrogation by law enforcement. Law enforcement's use of social media analysis may be cross-referenced with interrogation of portable IoT devices belonging to individuals who are suspected of attending protests [84, 85].

Hypothetical consequences. This chills the press by creating a fear of identification and reprisals both among sources and journalists gathering information on the ground [85].

Predictive analysis of location data to facilitate physical attacks. Tracking of a journalist or source by accessing the real-time geographic data gathered by and streamed from their car, fitness tracker or smart watch could also allow an adversary to infer previous routes and locations, or predict future ones [79, 86, 87].

Hypothetical consequences. This location information could be capitalised on to facilitate a physical attack [37, 87], or to implicate the journalist in a crime.

4.5 Data and device modification threats

The continued existence of a free press depends on journalists' dissemination of accurate information. If this is threatened, such as through alteration of data held on or proliferated by journalists' devices or accounts, it could discredit the work of entire news organisations and lower public trust in the news media. Additionally, sometimes consumer IoT devices have sufficiently intrusive intended functionalities that an adversary can use existing capabilities in ways that the user may not have intended, endangering the psychological and physical safety and security of a journalist or source.

Sensor-level attacks on data confidentiality or integrity. Information can be changed via Information Damage Level attacks, which relate to the sensors in IoT devices. These attacks can take different forms, usually involving monitoring, intercepting, modifying, fabricating or replicating data collected by these sensors and sent through a network. They particularly affect data confidentiality and integrity, as messages can be altered or recorded and replayed to the wrong people or at the wrong times [30].

Hypothetical consequences. These attacks could prevent journalists from feeling confident that they can effectively protect source information and that their work is founded in verifiable data.

Altering user-facing device and data attributes. Attacks used to alter user-facing information displayed on IoT devices could create psychological pressures that derail and undermine journalistic work, compromising journalists' reputations.

Hypothetical consequences. If an adversary overrides a photojournalist's authentication on a camera-equipped drone, this could prevent footage from being accessed and used. Spoofing data packets would cause devices to stop, start, or modify actions [43]. As a result, a journalist using a smart watch, for example, could be left unaware of messages that have been urgently sent to their phone by a source. Journalists often receive threatening messages [88], which could also be delivered through their devices, such as a voice assistant. If these two events coincide, there is likely to be a chilling effect as they question the security of their professional systems and their own perceptions due to gaslighting [89, 90]. Another example is clock skewing: if an adversary can control the pulse-accurate, synchronised clocks in a broadcast station, they can stop a live programme from going out. Further, falsification of time stamps could make journalists' task of verification of sources much more difficult, which may then allow their conclusions to be debunked and their reputations to suffer, for example if a faked timestamp is used to evidence a story that a politician knew about an action prior to its occurrence, the journalist breaking the story could appear biased. Finally, digital forensics, which is already notoriously unreliable regarding consumer IoT devices, may be made more challenging because, for example, monitoring when specific actions have been taken could be hindered if time stamps can be easily falsified by changing the time on the device's clock [14].

Hijacking connected social media and communications accounts. Some smart White Goods have the ability to post from users' social media accounts or send emails [91], and hacking into a journalist's fridge and accessing their social media accounts in order to imitate them could be used for a variety of nefarious purposes [92–94].

Hypothetical consequences. If a consumer IoT device that has access to a journalist's social media accounts is hacked and an adversary is able to publish disinformation under a journalist's name from their own account [95], that would likely undermine the journalist's credibility. If this process repeats, the journalist's audience could shift or disappear to such an extent that the journalist no longer has a following of note or a sufficiently good reputation to have standing within the industry. The advent of global digital media platforms has created an environment with huge public influence and little regulation. Even democratic governments are using the disinformation crisis to pass more subversively restrictive laws on journalism with the pretext of inhibiting the spread of disinformation [96]. This could be used as evidence to invoke laws that would then result in the prosecution of the journalist.

Manipulation of devices' physical activities. Malware may change device settings and alter the behaviour or functionality of a device without the device owner's recognition. This can facilitate both clandestine surveillance and kinetic attacks in technologies from small consumer IoT devices to core national infrastructure, as happened with the Stuxnet hack [97].

Hypothetical consequences. Examples range from large-scale kinetic attacks against IoT devices that control public goods in an urban area where lots of news organisations are concentrated [30], to attacks on individual targets, such as remote takeovers of internet-connected vehicles resulting in adversaries gaining control of vital functions such as steering and braking [87], which could be used to physically harm journalists and sources [66, 98]. This kind of manipulation of the settings of devices with physical functionalities upon which a journalist relies, can range from these more urgently relevant examples, to having an indefinite timeframe, such as altering the temperature control function of a journalist's smart fridge so that it overcorrects, thereby spoiling the contents and poisoning the journalist [99].

4.6 Networked devices threats

The combination of multiple devices into IoT ecosystems presents unique challenges, meaning that Computer Network Exploitation (i.e. "hacking") of networks of Internet of Things devices can culminate in much greater harm than that posed by any single device [47, 100]. Smart hubs that coordinate devices can be attacked in a variety of ways, and can be used for Elevation of Privilege attacks, therefore giving adversaries high-level access to and control of connected IoT devices [43]. Due to poor encryption and the networked nature of the Internet of Things, an entire network of journalists' devices could be compromised if an adversary has access to just one IoT device [30]. Representatives of intelligence agencies of democratic states have openly stated their intention to use poorly secured IoT devices to pivot into a network and gather data on users [101], including credentials that would give them access to more secure systems [102]; these systems could include those belonging to news organisations.

Voice stealing. The ability to identify IoT devices present in an individual's home through open-source investigations is the first step to many different attacks, including active access-level attacks that are specific to voice assistants, such as "voice squatting in which an attack skill carries a phonetically similar invocation name to that of its target skill" and "word squatting where the attack invocation name includes the target's name and some strategically selected additional words" [4]. This was demonstrated when the UK's National Cyber Security Centre used a vulnerability in an IoT doll to unlock a smart door lock [103].

Hypothetical consequences. Due to the poor inbuilt security of IoT devices, there have already been recorded instances of accidental malfunction, such as when voice assistants have recorded more audio data than intended and have sent this to members of the user's contacts list [30, 80, 104]. If this occurs in a space where an editorial team is discussing an as-yet-unbroken story, the subject of the story could be directly or indirectly alerted. Further, intentional rerouting attacks such as voice stealing manipulate the data received by either end of a communications channel, and would be particularly problematic for journalist-source communication, or even for different members of a newsroom team discussing a sensitive story [14, 30]. This could also be used to tell devices to activate functions that might endanger physical safety; for a

journalist who has done public interviews, manipulation of the audio from those interviews to record a command that can then be played when an adversary calls the journalist's home phone, to activate a voice assistant, e.g. turning on ovens at night, to set fires in a journalist's home.

Denial of Service attacks. Denial of Service attacks can be effected against Internet of Things devices if a device's availability is maliciously overloaded through unnecessary data traffic [14]. This can be particularly damaging if the device has an essential function, such as monitoring blood sugar or pulse [58]. DoS could be achieved by exploiting vulnerabilities in the hub to disrupt the entire smart home ecosystem [14, 30, 43]. Being targeted by DoS attacks reduces a network's capacity and can disable it, which could occur if an adversary exhausts the resources of a specific IoT device or network by overloading communications or overusing a specific functionality. This could then cause the device to shut down due to low power, which would be particularly problematic if it is a device that centrally coordinates other IoT devices thus impacting the wider network [30]. Given the range of functionalities that consumer IoT devices can possess, users may come to rely on them, triggering detrimental physical and psychological effects if device functionality is unexpectedly limited [58, 105]. Disruption of technological networks and denial of internet access are already features of governments' toolboxes [106], intended to prevent communication either to, by or among specific groups [107], and so it stands to reason that this would be extended to situations involving IoT devices, making this a likely category of threats to be enacted.

Hypothetical consequences. If a journalist is reliant on the availability of a specific network or device that can be accessed through an insecure IoT device, DoS (e.g. through Information Damage Level attacks) could leave them vulnerable to extortion [14, 43]. Similarly, restriction of internet access could have a particularly negative impact on journalists who are using such devices to report, such as camera-equipped drones. Internet-access denial tactics are also used to reinforce aggressive treatment of journalists covering protests by preventing them from using portable IoT devices to report on the ground.

5 Discussion

Section 4 answered both research questions by identifying the distinctive and novel threats to journalism from the consumer IoT and categorising them in a way that is easily comprehensible by journalists. Section 5 is a commentary on the implications of answering these questions.

5.1 What are the distinctive and novel threats to journalism from the consumer IoT?

The literature review and synthesis conducted for this research determined that, although there is ample evidence that IoT devices are capable of these threats, this is

not communicated in journalist-facing publications. Rather, it remains siloed in two forms; in heavily technical academic papers, or in resources created by organisations that support survivors of intimate partner violence (IPV) [41, 108]. In the latter case, while the information on IoT threats is conveyed in a way that is accessible to non-technical audiences, it is not presented to journalists as also relevant to them, nor is there much discussion of the potential for targeted exploitation outside IPV scenarios.

Additionally, legal and non-legal threat categories can overlap if journalists are reluctant to report IoT breach issues to law enforcement. This could be due to credibility worries, data privacy concerns, or because police violence and indifference towards public violence against journalists has featured heavily in the news [109].

5.2 How can we categorise these threats in a way that is easily comprehensible by journalists?

The specialist nature of these different research communities enables in-depth studies into the security and privacy flaws inherent in the consumer IoT. There are also transdisciplinary discussions and studies conducted that involve experts in topics such as privacy, surveillance, cyber security and the IoT. However, their segregation from non-specialist media means that not just the press, but also other highly targeted groups, are underserved.

This new categorisation contributes to this area of research in two ways. First, it presents clear descriptions and examples of all threats, whether they're regulatory and legal, threats relating to both technical manipulation, or human threats such as profiling and tracking. Second, it brings the IoT into journalism-specific cyber security considerations. These changes allow this article to be used to increase journalists' awareness of potential threats, regardless of their level of technical or legal knowledge.

5.3 Challenging areas and known unknowns

With this categorisation, areas of ambiguity arose because scenarios involved converging technologies or combined attack motivations and outcomes. A limitation of this research is that IoT threat modelling is nascent, compounded by the fact that other intrusive technologies (e.g. biometrics, deep fakes, facial recognition, etc.) are emerging alongside the development of the consumer IoT, which all intersect to facilitate unforeseen threats [64]. While we mention this overlap, it remains an underexplored area within the broader field.

Journalists are largely unaware of IoT threats and therefore the more clandestine threat scenarios that are explored in this work may go unreported, as journalists are gaslighted or do not realise that they are occurring [5, 90].

Further, state actors, such as security and intelligence agencies, often do not disclose the full extent of their capabilities regarding computer network exploitation [64, 110]. There are therefore 'unknown unknowns' relating to IoT threat modelling which means there are currently gaps in this categorisation. Nevertheless, the goal of this research is to be iterative and thus will continue to expand as this field expands.

Although the objective for this IoT threat model categorisation is to accurately classify journalists' IoT threat landscape, it could also highlight to IoT manufacturers the potential real-world impacts of their products' vulnerabilities. This would be a welcome outcome, as a recent study demonstrated that the fundamental cyber security built into IoT products has not only not improved but also that standards are slipping [94].

5.4 Future work

This article is also intended to inform subsequent studies by presenting threat models that are targeted at this specific user group. In particular, the language for discussing as-yet unmanifested threats tends to be aggressive, invoking fear that can be debilitating [111, 112]. Our paper intends to subvert that pattern by presenting threats with snapshots of hypothetical consequences that communicate both the device capabilities and the stakes involved in possible escalation of the threats. Our novel threat categorisation that is accessible to journalists will be operationalised to provide a foundation for our forthcoming recommendations for minimising and mitigating these threats to journalists.

6 Conclusion

Our research synthesised relevant literature across a range of disciplines and media to establish an understanding of the state of IoT and journalism threat modelling, IoT privacy threats and IoT material threats. This enabled the creation of exploratory threat scenarios in which the consumer IoT could be used to harm press freedom, mainly by attacking journalists' work and wellbeing.

These scenarios were thematically coded and analysed, to cluster and classify consumer IoT threats to privacy and security, as well as journalists' concerns. This formed our novel work, structured into six overarching exploratory categories: (1) regulatory gaps, (2) legal threats, (3) profiling threats, (4) tracking threats, (5) data and device modification threats, and (6) networked devices threats. Each delineates a category of IoT threat that has the potential to hamper journalistic work, with associated threats and example scenarios that describe potential consequences for the press. The choice to present the threat models in this format was taken to demonstrate that, far from being conceptual black swan scenarios, these threats are clearly feasible given today's IoT capabilities and the motivations of the highly resourced attackers who are likely to be targeting journalists. Additionally, given the prevalence and perceived inescapability of the consumer IoT [5], these threats against journalists are growing.

Acknowledgements

This work was supported by the Engineering and Physical Sciences Research Council under Grant EP/P00881X/1.

With thanks to Dr. Miranda Melcher, Dr. Jean Debarros and Jonathan Foldi for their invaluable help, support and encouragement. Thanks also to the Cyber Science 2022 reviewers for their useful feedback.

References

1. Barbosa, N.M., Zhang, Z., Wang, Y.: Do Privacy and Security Matter to Everyone? Quantifying and Clustering User-Centric Considerations About Smart Home Device Adoption. In: Proceedings of the Sixteenth USENIX Symposium on Usable Privacy and Security. pp. 417–435. USENIX Association, Virtual (2020)
2. Nurse, J., Erola, A., Agrafiotis, I., Goldsmith, M., Creese, S.: Smart Insiders: Exploring the Threat from Insiders Using the Internet-of-Things. In: Proceedings of the 2015 International Workshop on Secure Internet of Things (SIoT). , Vienna, Austria (2015)
3. Tanczer, L.M., Steenmans, I., Elsdén, M., Blackstock, J., Carr, M.: Emerging risks in the IoT ecosystem: Who’s afraid of the big bad smart fridge? In: Living in the Internet of Things: Cybersecurity of the IoT - 2018. p. 33 (9 pp.)-33 (9 pp.). Institution of Engineering and Technology, London, UK (2018)
4. Zhang, N., Mi, X., Feng, X., Wang, X., Tian, Y., Qian, F.: Dangerous Skills: Understanding and Mitigating Security Risks of Voice-Controlled Third-Party Functions on Virtual Personal Assistant Systems. In: 2019 IEEE Symposium on Security and Privacy (SP). pp. 1381–1396. IEEE, Stockholm, Sweden (2019)
5. Shere, A.R.K., Nurse, J.R.C., Flechais, I.: ‘Security should be there by default’: Investigating how journalists perceive and respond to risks from the Internet of Things. Presented at the 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) September 1 (2020)
6. Phillips, G.: How the free press worldwide is under threat, <https://www.theguardian.com/media/2020/may/28/how-the-free-press-worldwide-is-under-threat>, (2020)
7. The Nobel Prize: The Nobel Peace Prize 2021, <https://www.nobelprize.org/prizes/peace/2021/press-release/>
8. Ball, J.: GCHQ captured emails of journalists from top international media, <https://www.theguardian.com/uk-news/2015/jan/19/gchq-intercepted-emails-journalists-ny-times-bbc-guardian-le-monde-reuters-nbc-washington-post>, (2015)
9. Pegg, D., Lewis, P., Safi, M., Lakhani, N.: FT editor among 180 journalists identified by clients of spyware firm, <https://www.theguardian.com/world/2021/jul/18/ft-editor-roula-khalaf-among-180-journalists-targeted-nso-spyware>, (2021)
10. Woodhams, S.: Spyware: An Unregulated and Escalating Threat to Independent Media, <https://www.cima.ned.org/publication/spyware-an-unregulated-and-escalating-threat-to-independent-media/>, (2021)
11. Pickard, V.: Restructuring Democratic Infrastructures: A Policy Approach to the Journalism Crisis. *Digital Journalism*. 8, 704–719 (2020). <https://doi.org/10.1080/21670811.2020.1733433>


12. Stotzky, I.P.: The Role of a Free Press and Freedom of Expression in Developing Democracies. *U. Miami L. Rev.* 56, 255 (2001)
13. Council of Europe: The 2019 Annual Report by the partner organisations of the Council of Europe's Platform for the Protection of Journalism and Safety of Journalists: 'Democracy at Risk: threats and attacks against media freedom in Europe'. Council of Europe, Council of Europe, Avenue de l'Europe F-67075 Strasbourg Cedex, France (2019)
14. Gulzar, M., Abbas, G.: Internet of Things Security: A Survey and Taxonomy. In: 2019 International Conference on Engineering and Emerging Technologies (ICEET). pp. 1–6. IEEE, Lahore, Pakistan (2019)
15. Zorz, Z.: Government-backed cyber attackers increasingly targeting journalists, <https://www.helpnetsecurity.com/2020/03/27/cyber-attackers-targeting-journalists/>, (2020)
16. Crete-Nishihata, M., Oliver, J., Parsons, C., Walker, D., Tsui, L., Deibert, R.: The Information Security Cultures of Journalism. *Digital Journalism*. 0, 1–24 (2020). <https://doi.org/10.1080/21670811.2020.1777882>
17. McGregor, S.E., Charters, P., Holliday, T., Roesner, F.: Investigating the Computer Security Practices and Needs of Journalists. In: Proceedings of the 24th USENIX Security Symposium. p. 17. USENIX Association, Washington, D.C. (2015)
18. McGregor, S.E., Watkins, E.A., Al-Ameen, M.N., Caine, K., Roesner, F.: When the Weakest Link is Strong: Secure Collaboration in the Case of the Panama Papers. In: Proceedings of the 26th USENIX Security Symposium. p. 19. USENIX Association, Vancouver, BC, Canada (2017)
19. McGregor, S.E., Watkins, E.A.: "Security by Obscurity": Journalists' Mental Models of Information Security. *#ISOJ*. 6, (2016)
20. Uzunov, A.V., Fernandez, E.B.: An extensible pattern-based library and taxonomy of security threats for distributed systems. *Computer Standards & Interfaces*. 36, 734–747 (2014). <https://doi.org/10.1016/j.csi.2013.12.008>
21. Electronic Frontier Foundation: Threat model, <https://ssd.eff.org/en/glossary/threat-model>
22. Fruhlinger, J.: Threat modeling explained: A process for anticipating cyber attacks, <https://www.csoonline.com/article/3537370/threat-modeling-explained-a-process-for-anticipating-cyber-attacks.html>
23. Torr, P.: Demystifying the threat modeling process. *IEEE Security Privacy*. 3, 66–70 (2005). <https://doi.org/10.1109/MSP.2005.119>
24. Xiong, W., Lagerström, R.: Threat modeling – A systematic literature review. *Computers & Security*. 84, 53–69 (2019). <https://doi.org/10.1016/j.cose.2019.03.010>
25. Bradshaw, P.: Why every journalist should have a threat model (with cats), <https://onlinejournalismblog.com/2014/07/16/why-every-journalist-should-have-a-threat-model-with-cats/>, (2014)
26. Stray, J.: Security for Journalists, Part Two: Threat Modeling, <https://source.opennews.org/articles/security-journalists-part-two-threat-modeling/>

27. Szathmari, G.: Threats | Threat Modeling | Privacy for Journalists, <https://privacyforjournalists.org.au/threat-modeling-for-journalists>
28. Rory Peck Trust: Digital Risk Assessment, <https://rorypecktrust.org/resources/Digital-Security-Guide/Digital-Risk-Assessment?cu=en-GB>
29. Herrman, J.: The Tools for Covering Tech Are the Same as in 2009, <https://www.nytimes.com/2019/07/31/technology/personaltech/tools-covering-tech-same-2009.html>, (2019)
30. Nawir, M., Amir, A., Yaakob, N., Lynn, O.B.: Internet of Things (IoT): Taxonomy of security attacks. In: 2016 3rd International Conference on Electronic Design (ICED). pp. 321–326. IEEE, Phuket, Thailand (2016)
31. Alrawi, O., Lever, C., Antonakakis, M., Monroe, F.: SoK: Security Evaluation of Home-Based IoT Deployments. In: 2019 IEEE Symposium on Security and Privacy (SP). pp. 1362–1380. IEEE, San Francisco, CA, USA (2019)
32. Perez, A.J., Zeadally, S., Griffith, S.: Bystanders’ Privacy. *IT Professional*. 19, 61–65 (2017). <https://doi.org/10.1109/MITP.2017.42>
33. Lopez, J., Rios, R., Bao, F., Wang, G.: Evolving privacy: From sensors to the Internet of Things. *Future Generation Computer Systems*. 75, 46–57 (2017). <https://doi.org/10.1016/j.future.2017.04.045>
34. Goulden, M., Tolmie, P., Mortier, R., Lodge, T., Pietilainen, A.-K., Teixeira, R.: Living with interpersonal data: Observability and accountability in the age of pervasive ICT. *New Media & Society*. 20, 1580–1599 (2018). <https://doi.org/10.1177/1461444817700154>
35. Christensen, A.T., Olesen, H., Sørensen, L.: On the Value of the Counterfactual and How the Smart Home Informs It. *Surveillance & Society*. 19, 241–243 (2021). <https://doi.org/10.24908/ss.v19i2.14301>
36. Burdon, M., Cohen, T.: Modulation Harms and The Google Home. *Surveillance & Society*. 19, 154–167 (2021). <https://doi.org/10.24908/ss.v19i2.14299>
37. Cha, S.-C., Hsu, T.-Y., Xiang, Y., Yeh, K.-H.: Privacy Enhancing Technologies in the Internet of Things: Perspectives and Challenges. *IEEE Internet of Things Journal*. 6, 2159–2187 (2019). <https://doi.org/10.1109/JIOT.2018.2878658>
38. Kazansky, B.: ‘It depends on your threat model’: the anticipatory dimensions of resistance to data-driven surveillance. *Big Data & Society*. 8, 2053951720985557 (2021). <https://doi.org/10.1177/2053951720985557>
39. Heartfield, R., Loukas, G., Budimir, S., Bezemskij, A., Fontaine, J.R.J., Filippopolitis, A., Roesch, E.: A taxonomy of cyber-physical threats and impact in the smart home. *Computers & Security*. 78, 398–428 (2018). <https://doi.org/10.1016/j.cose.2018.07.011>
40. Blythe, J.M., Johnson, S.D.: A systematic review of crime facilitated by the consumer Internet of Things. *Secur J.* (2019). <https://doi.org/10.1057/s41284-019-00211-8>
41. Lopez-Neira, I., Patel, T., Parkin, S., Danezis, G., Tanczer, L.: ‘Internet of Things’: How Abuse is Getting Smarter. Social Science Research Network, Rochester, NY (2019)

42. Chalhoub, G., Flechais, I., Nthala, N., Abu-Salma, R.: Innovation Inaction or In Action? The Role of User Experience in the Security and Privacy Design of Smart Home Cameras. In: Proceedings of the Sixteenth USENIX Symposium on Usable Privacy and Security. p. 21. USENIX Association, Virtual (2020)
43. Hoffmann, S.: IoT Security Architecture and Policy for the Home - a Hub Based Approach. IoT Security Foundation, Oxford, United Kingdom (2018)
44. Atamli, A.W., Martin, A.: Threat-Based Security Analysis for the Internet of Things. In: 2014 International Workshop on Secure Internet of Things. pp. 35–43 (2014)
45. PRISMA: Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) Checklist, <http://prisma-statement.org/PRISMAStatement/Checklist.aspx>
46. Rasmussen, L.B.: The narrative aspect of scenario building - How story telling may give people a memory of the future. *AI & Soc.* 19, 229–249 (2005). <https://doi.org/10.1007/s00146-005-0337-2>
47. Kebande, V.R., Karie, N.M., Michael, A., Malapane, S.M.G., Venter, H.S.: How an IoT-enabled “smart refrigerator” can play a clandestine role in perpetuating cyber-crime. In: 2017 IST-Africa Week Conference (IST-Africa). pp. 1–10 (2017)
48. Freund, J.: Threat-Modeling Basics Using MITRE ATT&CK, <https://www.darkreading.com/risk/threat-modeling-basics-using-mitre-attandck/a/d-id/1337728>
49. Kenyon, M.: Dubious Denials & Scripted Spin: Spyware Company NSO Group Goes on 60 Minutes, <https://citizenlab.ca/2019/04/dubious-denials-scripted-spin-spyware-company-nso-group-goes-on-60-minutes/>, (2019)
50. Rueckert, P.: Pegasus: The new global weapon for silencing journalists, <https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/>, (2021)
51. Scott-Railton, J., Marczak, B., Razzak, B.A., Crete-Nishihata, M., Deibert, R.: Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware. University of Toronto, The Citizen Lab (2017)
52. Lindsay, G., Woods, B., Corman, J.: Issue Brief: Smart Homes and the Internet of Things. The Atlantic Council: the Brent Scowcroft Center on International Security, Washington, D.C. (2016)
53. Meteriz, Ü., Fazıl Yilduran, N., Kim, J., Mohaisen, D.: Understanding the Potential Risks of Sharing Elevation Information on Fitness Applications. In: 2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS). pp. 464–473 (2020)
54. Hassan, W.U., Hussain, S., Bates, A.: Analysis of Privacy Protections in Fitness Tracking Social Networks -or- You can run, but can you hide? Presented at the 27th USENIX Security Symposium (USENIX Security 18) (2018)
55. Sadowski, J.: When data is capital: Datafication, accumulation, and extraction. *Big Data & Society.* 6, 2053951718820549 (2019). <https://doi.org/10.1177/2053951718820549>
56. Käll, J.: The Materiality of Data as Property. *Harvard International Law Journal.* 61, 1–11 (2020)

57. Michel, M.C.K., King, M.C.: Cyber Influence of Human Behavior: Personal and National Security, Privacy, and Fraud Awareness to Prevent Harm. In: 2019 IEEE International Symposium on Technology and Society (ISTAS). pp. 1–7. IEEE, Medford, MA, USA (2019)
58. Anell, S., Grober, L., Krombholz, K.: End User and Expert Perceptions of Threats and Potential Countermeasures. In: The 5th European Workshop on Usable Security. p. 10. IEEE, Genova, Italy (2020)
59. Krebs, B.: KrebsOnSecurity Hit With Record DDoS — Krebs on Security, <https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/>, (2016)
60. Tabassum, M., Kosiński, T., Lipford, H.R.: ‘I don’t own the data’: end user perceptions of smart home device data practices and risks. In: Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security. pp. 435–450. USENIX Association, USA (2019)
61. Wright, L.: Economic Espionage and Business Intelligence. In: Wright, L. (ed.) People, Risk, and Security: How to prevent your greatest asset from becoming your greatest liability. pp. 91–105. Palgrave Macmillan UK, London (2017)
62. Rizvi, S., Kurtz, A., Pfeffer, J., Rizvi, M.: Securing the Internet of Things (IoT): A Security Taxonomy for IoT. In: 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). pp. 163–168 (2018)
63. Cimpanu, C.: A Massive Botnet of CCTV Cameras Involved in Ferocious DDoS Attacks, <https://news.softpedia.com/news/a-massive-botnet-of-cctv-cameras-involved-in-ferocious-ddos-attacks-505722.shtml>, (2016)
64. Smith, S.: The Internet of Risky Things: Trusting the Devices That Surround Us. O’Reilly Media, Inc., Sebastopol, CA, USA (2017)
65. McGregor, S.: Why DDoS attacks matter for journalists, https://www.cjr.org/tow_center/journalists_ddos_hack_passwords.php
66. Agrafiotis, I., Nurse, J.R.C., Goldsmith, M., Creese, S., Upton, D.: A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *J Cyber Secur.* 4, (2018). <https://doi.org/10.1093/cybsec/tyy006>
67. Holcomb, J., Mitchell, A., Page, D.: Investigative journalists and digital security: Perceptions of vulnerability and changes in behavior. Pew Research Center in association with Columbia University’s Tow Center for Digital Journalism, Columbia University, New York (2015)
68. Brevini, B.: Metadata Laws, Journalism and Resistance in Australia. *Media and Communication.* 5, 76–83 (2017). <https://doi.org/10.17645/mac.v5i1.810>
69. Information Commissioner’s Office: Data Protection Act 2018: For Organisations, <https://ico.org.uk/for-organisations/data-protection-act-2018/>
70. Shere, A.R.K.: Now you [don’t] see me: how have new legislation and changing public awareness of the UK surveillance state impacted OSINT investigations? *Journal of Cyber Policy.* 5, 429–448 (2020). <https://doi.org/10.1080/23738871.2020.1832129>

71. Pavur, J., Knerr, C.: GDPArrrr: Using Privacy Laws to Steal Identities. In: Blackhat USA 2019 Whitepaper. p. 10. Blackhat USA, Las Vegas (2019)
72. Frost, J., Hamlin, A.: Ransomware - A Strategic Threat to Organizations. *Mountain Plains Journal of Business and Technology*. 21, (2020)
73. Solove, D.J., Hartzog, W.: *Breached!: Why Data Security Law Fails and How to Improve it*. Oxford University Press, Oxford, New York (2022)
74. Cox, J.: Customs and Border Protection Paid \$476,000 to a Location Data Firm in New Deal, https://www.vice.com/en_ca/article/k7qyv3/customs-border-protection-venntel-location-data-dhs
75. Cox, J.: The Loophole the DMV Uses to Sell Your Data to Private Investigators, https://www.vice.com/en_us/article/ep47na/dmv-dppa-drivers-privacy-protection-act-buy-data-private-investigators, (2020)
76. Aksu, H., Babun, L., Conti, M., Tolomei, G., Uluagac, A.S.: Advertising in the IoT Era: Vision and Challenges. *arXiv:1802.04102 [cs]*. (2018)
77. Rahaman, T.: Smart Things are Getting Smarter: An Introduction to the Internet of Behavior. *Medical Reference Services Quarterly*. 41, 110–116 (2022). <https://doi.org/10.1080/02763869.2022.2021046>
78. Abdi, N., Ramokapane, K.M., Such, J.M.: More than smart speakers: security and privacy perceptions of smart home personal assistants. In: *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security*. pp. 451–466. USENIX Association, USA (2019)
79. Alqhatani, A., Lipford, H.R.: ‘There is nothing that i need to keep secret’: sharing practices and concerns of wearable fitness data. In: *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security*. pp. 421–434. USENIX Association, USA (2019)
80. Edu, J.S., Such, J.M., Suarez-Tangil, G.: Smart Home Personal Assistants: A Security and Privacy Review. *arXiv:1903.05593 [cs]*. (2019)
81. Liverpool, L.: Voice assistant recordings could reveal what someone nearby is typing, <https://www.newscientist.com/article/2261844-voice-assistant-recordings-could-reveal-what-someone-nearby-is-typing/>, (2020)
82. Sturgess, J., Nurse, J.R.C., Zhao, J.: A capability-oriented approach to assessing privacy risk in smart home ecosystems. In: *2018 IET PETRAS Living in the Internet of Things: Cybersecurity of the IoT - 2018*. p. 37 (8 pp.)-37 (8 pp.). Institution of Engineering and Technology, London, UK (2018)
83. Wakefield, J.: Ring doorbells to send live video to Mississippi police, <https://www.bbc.com/news/technology-54809228>, (2020)
84. Shere, A.R.K., Nurse, J.R.C.: Police surveillance of Black Lives Matter shows the danger technology poses to democracy, <http://theconversation.com/police-surveillance-of-black-lives-matter-shows-the-danger-technology-poses-to-democracy-142194>, (2020)
85. Access Now: New world disorder: digital attacks on freedom of assembly, <https://www.accessnow.org/new-world-disorder-digital-attacks-on-freedom-of-assembly/>, (2020)
86. @DFRLab: Data and Defense: The Case of Strava, <https://medium.com/dfrlab/data-and-defense-the-case-of-strava-6b56ee3b1a2>

87. National Security Agency: Limiting Location Data Exposure. National Security Agency, USA (2020)
88. Binns, A.: Fair game? Journalists' experiences of online abuse. *Journal of Applied Journalism & Media Studies*. 6, 183–206 (2017). https://doi.org/10.1386/ajms.6.2.183_1
89. Middleton, L.: Woman 'hacked into ex-boyfriend's Alexa and told his new girlfriend to leave', <https://metro.co.uk/2020/10/12/woman-hacked-into-ex-boyfriends-alexa-and-told-his-new-girlfriend-to-leave-13407458/>, (2020)
90. Moody, G.: The enemy within: welcome to the Internet of gaslighting, <https://www.privateinternetaccess.com/blog/the-enemy-within-welcome-to-the-internet-of-gaslighting/>
91. Agence France-Presse (AFP): Hackers use 'smart' refrigerator to send 750,000 virus-laced emails, <https://www.rawstory.com/2014/01/hackers-use-smart-refrigerator-to-send-750000-virus-laced-emails/>, (2014)
92. Greenberg, A.: Hackers Broke Into Real News Sites to Plant Fake Stories, <https://www.wired.com/story/hackers-broke-into-real-news-sites-to-plant-fake-stories-anti-nato/>, (2020)
93. Hamilton, E.: Eric Hamilton on Twitter: 'Here's a thing that happened today. I was recently -- and falsely -- linked to an article I didn't write, because the author who DID write it happens to share the same name/byline as I do. I'm not going to link to it because it's complete garbage.', <https://twitter.com/OnetheycallEric/status/1270857748092239872>
94. Honeywell, L.: Leigh Honeywell @  on Twitter: 'Btw this Eric Hamilton is _not_ the author of the shitty stalker article, just has the misfortune of the same name and profession', <https://twitter.com/hypatiadotca/status/1270978645327110145>
95. Schwedel, S., Palus, H.: A Ranking of the Weirdest Appliances That You Can Technically Tweet From, <https://slate.com/technology/2019/08/twitter-electronics-ranked-list-which-is-best.html>
96. Reporters Without Borders: RSF unveils 20/2020 list of press freedom's digital predators | Reporters without borders, <https://rsf.org/en/news/rsf-unveils-202020-list-press-freedoms-digital-predators>
97. Patel, C., Doshi, N.: Security Challenges in IoT Cyber World. In: Hassanien, A.E., Elhoseny, M., Ahmed, S.H., and Singh, A.K. (eds.) *Security in Smart Cities: Models, Applications, and Challenges*. pp. 171–191. Springer International Publishing, Cham (2019)
98. Staff of Senator Ed Markey: Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk. Office of the United States Senator for Massachusetts, Massachusetts, USA (2015)
99. Bhartiya, S.: Your smart fridge may kill you: The dark side of IoT, <https://www.infoworld.com/article/3176673/your-smart-fridge-may-kill-you-the-dark-side-of-iot.html>
100. Nassi, B., Bitton, R., Masuoka, R., Shabtai, A., Elovici, Y.: SoK: Security and Privacy in the Age of Commercial Drones. Presented at the 2021 IEEE Symposium on Security and Privacy (SP) (2021)

101. McLaughlin, J.: NSA Looking to Exploit Internet of Things, Including Biomedical Devices, Official Says, <https://theintercept.com/2016/06/10/nsa-looking-to-exploit-internet-of-things-including-biomedical-devices-official-says/>, (2016)
102. Ackerman, S., Thielman, S.: US intelligence chief: we might use the internet of things to spy on you, <https://www.theguardian.com/technology/2016/feb/09/internet-of-things-smart-home-devices-government-surveillance-james-clapper>, (2016)
103. Levy, I.: Hacked doll 'could open front door', <https://www.bbc.co.uk/news/av/technology-38966285>, (2017)
104. Shaban, H.: An Amazon Echo recorded a family's conversation, then sent it to a random person in their contacts, report says - The Washington Post, <https://www.washingtonpost.com/news/the-switch/wp/2018/05/24/an-amazon-echo-recorded-a-familys-conversation-then-sent-it-to-a-random-person-in-their-contacts-report-says/>, (2018)
105. Finley, K.: Why Tech's Best Minds Are Very Worried About the Internet of Things, <https://www.wired.com/2014/05/iot-report/>, (2014)
106. Mahase, E.: Kashmir communications blackout is putting patients at risk, doctors warn. *BMJ*. 366, 15204 (2019). <https://doi.org/10.1136/bmj.15204>
107. Elliott, V.: Four ways governments disrupt internet access, <https://restofworld.org/2021/four-ways-governments-disrupt-internet-access/>
108. Tanczer, L.: Gender and the Internet of Things ('IoT'): Futureproofing Online Harms legislation. UCL Department of Science, Technology, Engineering and Public Policy (UCL STEaPP), London, UK (2020)
109. Reporters Without Borders: 2020 World Press Freedom Index: "Entering a decisive decade for journalism, exacerbated by coronavirus" | RSF, <https://rsf.org/en/2020-world-press-freedom-index-entering-decisive-decade-journalism-exacerbated-coronavirus>
110. Deutsche Welle: Morocco arrests journalist on rape and spy charges, <https://www.dw.com/en/omar-radi-morocco-journalist/a-54372595>
111. Cap, P.: *The Language of Fear: Communicating Threat in Public Discourse*. Springer, London, UK (2016)
112. Lawson, S.: Putting the "war" in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States. *First Monday*. 17, (2012). <https://doi.org/10.5210/fm.v17i7.3848>