University of Kent

Kent Academic Repository

Shere, Anjuli R. K., Nurse, Jason R. C. and Martin, Andrew (2025) *The long, strong arm of the law: legal Internet of Things threats to journalists globally*. Journalism Practice . ISSN 1751-2786.

Downloaded from
https://kar.kent.ac.uk/108975/ The University of Kent's Academic Repository KAR

The version of record is available from
https://doi.org/10.1080/17512786.2025.2567435

This document version
Publisher pdf

DOI for this version

Licence for this version
CC BY (Attribution)

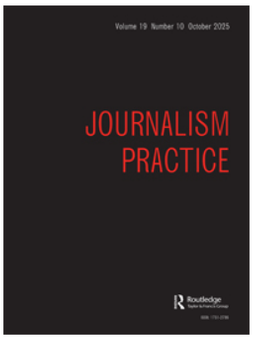
Additional information

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 (available from https://www.kent.ac.uk/guides/kar-the-kent-academic-repository#policies).



Routledge
Taylor & Francis Group

Journalism Practice

ISSN: 1751-2786 (Print) 1751-2794 (Online) Journal homepage: www.tandfonline.com/journals/rjop20

The Long, Strong Arm of the Law: Legal Internet of Things Threats to Journalists Globally

Anjuli R. K. Shere, Jason R. C. Nurse & Andrew P. Martin

To cite this article: Anjuli R. K. Shere, Jason R. C. Nurse & Andrew P. Martin (09 Oct 2025): The Long, Strong Arm of the Law: Legal Internet of Things Threats to Journalists Globally, Journalism Practice, DOI: 10.1080/17512786.2025.2567435

To link to this article: https://doi.org/10.1080/17512786.2025.2567435

© 2025 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group

Published online: 09 Oct 2025.

Submit your article to this journal

Article views: 26

View related articles

View Crossmark data

Full Terms & Conditions of access and use can be found at
https://www.tandfonline.com/action/journalInformation?journalCode=rjop20

JOURNALISM PRACTICE
https://doi.org/10.1080/17512786.2025.2567435

Routledge
Taylor & Francis Group

OPEN ACCESS Check for updates

The Long, Strong Arm of the Law: Legal Internet of Things Threats to Journalists Globally

Anjuli R. K. Shere[a], Jason R. C. Nurse[b] and Andrew P. Martin[a]

[a]Department of Computer Science, University of Oxford, Oxford, UK; [b]School of Computing, University of Kent, Canterbury, UK

ABSTRACT

The recent and rapid development of the consumer networked devices – Internet of Things (IoT) – market has led to the lawful collection of massive, diverse amounts of data. In asking the research question: "To what extent do existing laws and regulations in Taiwan, Australia, the UK and the US facilitate risk from the IoT to the media?", this paper compares and contrasts significant laws, their relevance to the IoT, and their impact on journalists' work and wellbeing in four democracies. Based on 63 interviews with journalists and relevant experts, this paper uses these case studies to provide a snapshot of domestic government overreach and inadequacy via legal means, which indicates a long-term issue of state agencies creating and abusing mechanisms in legislation to access data that could include information on journalists and their sources. This paper contributes to journalism studies and to the practice of journalism itself by exploring the legislative context that shapes press freedom in environments of continuous IoT surveillance and Big Data collation. The comparative analysis presented in this paper highlights the broader implications for democracy of legislation that either capitalises on or ignores the impact of IoT risks to journalistic work and source confidentiality.

ARTICLE HISTORY
Received 7 June 2024
Accepted 22 September 2025

KEYWORDS
Internet of Things (IoT); big data; surveillance; legislation; Taiwan; United Kingdom (UK); United States of America (USA); Australia

Introduction

Even in democratic countries, journalists must contend with declining political support, a growing number of technologies that enable data collection, and associated legal challenges (Phillips 2020). Many press freedom-focused civil society organisations and academics publish threat intelligence reports and guidance on protection from both conventional physical attacks and cyber security threats (Kenyon 2019; McGregor 2021; UNESCO 2015). Following the Snowden revelations regarding state-sponsored surveillance of the press (Ball 2015; Lashmar 2017; Russell et al. 2017), much of this advice addresses threats such as spying on traditional devices (phones, routers, laptops, tablets and desktop computers). However, very little of this literature mentions another

CONTACT Andrew P. Martin andrew.martin@cs.ox.ac.uk

© 2025 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group
This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

rapidly proliferating area of emerging technology that can facilitate threats similar to and beyond these examples: the consumer Internet of Things (IoT).

Consumer IoT devices have sensors that facilitate the collection of a range of types of data (Shere 2021), and all manner of non-users have accessed this information – from Amazon employing thousands of workers to listen to smart speaker recordings to train its proprietary Artificial Intelligence (Day, Turner, and Drozdiak 2019), to Israel's tracking of Hezbollah operatives using the operatives' own devices such as smart car odometers, drones, CCTV feeds and TV remote microphones (Srivastava et al. 2024). While news reports clearly demonstrate the vast capabilities of these devices, there are a number of areas in which new research is needed to understand how the IoT exacerbates and creates risks to the media. An initial study proved that journalists are widely unaware of the risks they face from the IoT, and that cyber security experts consider this lack of awareness to be problematic for ensuring journalistic safety (Shere, Nurse, and Flechais 2020). This paper builds on that work to ask the following research question: To what extent do existing laws and regulations in Taiwan, Australia, the UK and the US facilitate risk from the IoT to the media?

For this research, the IoT excludes the aforementioned traditional devices, because they pose well-known and well-studied threats (Blythe and Johnson 2021); however, it does include devices available to consumers that are able to connect to other devices or to the Internet, so they have functionalities that can be activated remotely (Nurse et al. 2015). Therefore, the term "IoT" in this article covers a range of devices from voice assistants (like Alexa and Google Home) to equipment that was not previously connected but has had this capability built into later models (like smart fridges and video-equipped doorbells).

This paper presents a multidisciplinary exploration into the complex interplay between journalism, cyber security, and contemporary geopolitical and legislative landscapes. Drawing upon insights from 63 expert interviews, news media analysis, and cyber security academic and industry literature, this study builds four detailed case study profiles of the legislative and relevant policy environments created and maintained by the governments in Taiwan, Australia, the United Kingdom and the United States regarding the extent to which IoT threats are perceived and mitigated in the news industry of each country. The results of these case studies and comparisons between them demonstrate that IoT-related threats to journalists come both directly from the devices, and from laws that either deliberately or practically allow the exploitation of these technologies to threaten press freedom, and therefore democracy.

The UK, the US, Taiwan and Australia are internationally influential liberal democracies (Thompson n.d.; Wells 2020), with English as a widely used media language (Tian, Liu, and Christian 2004), policymaker interest in developing and/or regulating the IoT market (Castro and New 2016; Department of Home Affairs n.d.; Department of Investment Service, Ministry of Economic Affairs n.d.; Gunashekar et al. 2016), and recent domestic data collection-related legislation (DLA Piper: Law in Australia n.d.; DLA Piper: Law in Taiwan, China n.d.; DLA Piper: Law in United States n.d.; Information Commissioner's Office 2018). The inclusion of Taiwan seems to be an outlier among countries that are typically Western democracies. However, Taiwan represents a different but equally valid class of emerging democracies with a demonstrated dedication to the values that stereotypically characterise such countries, in an era where such values are depleting in other, more established democratic nation-states.

This interdisciplinary approach not only enriches academic discourse within journalism studies and cyber security research, but policymakers will be able to compare the manifestation of certain threats and challenges across countries and derive insights about how to future-proof technological legislation without eroding journalistic protections.

Relevant Literature

Surveillance Studies

A large component of IoT risk relates to continual surveillance, which can be both facilitated and exacerbated by legislation. While Lashmar and Di Salvo both argue that surveillance of journalists is ever more pervasive and intrusive and is exacerbated by states outsourcing data collection to private companies (Di Salvo 2022; Lashmar 2020), little research explicitly considers the interaction between IoT and the law. Berger's article on the future of the press does consider the double-edged sword of massive data collection and how it may be exploited by actors who seek to harm the news industry. Still, even Berger only briefly mentioned that the media's infatuation with technology and Big Data could be accompanied by risks such as surveillance (Berger 2018). This research was therefore underpinned and motivated by theoretical frameworks from the three phases of surveillance theory explored by Galič et al. within the field of surveillance studies (Galič, Timan, and Koops 2017). These phases are: (1) centralised state-run panopticism, (2) surveillance networks that include non-state actors such as commercial entities and (3) continuous surveillance of many kinds, by many actors. Supporting the pertinence of all of these elements of surveillance theory to this research is the pilot study's finding that journalists are aware that the IoT is omnipresent and watching, thereby effectively chilling reporting (Lyon 2018; Shere, Nurse, and Flechais 2020).

The first phase, Bentham and Foucault's ideas of centralised and architectural panopticism, relate to this research because of the consistent threat of state overreach into journalists' affairs through IoT devices (Bentham 2012). The second phase, per Haggerty and Ericson, directly accounts for a "surveillance assemblage" of ubiquitous networked devices that exponentially increase the capacity for surveillance by actors beyond the state (Haggerty and Ericson 2000). Also characterised as part of the second phase of surveillance theory is Zuboff's theory of "surveillance capitalism" (Zuboff 2019). Burgess and Hurcombe noted that concentration of proprietary power in the hands of certain technology companies, and particularly social media platforms, has undermined journalists' capabilities "to use these kinds of digital methods for the purposes of public oversight of the digital media environment" (Burgess and Hurcombe 2019).

The third phase, which Galič et al. framed as reviewing mass surveillance by states, corporations, individuals, all separately and together, includes Clarke's "dataveillance" and Mann's "sousveillance" (Clarke 1988; Galič, Timan, and Koops 2017; Mann 2016). These ideas illustrate that IoT risk, particularly from data collection, is everywhere, all the time, and by all actors. Kazansky and Milan noted that civil society subverts the typical construct of surveillance producers and victims by attempting to expose the dangers and absurdity of such data collection, but that they can only do so in limited ways (Kazansky and Milan 2021).

How do States Regulate the IoT?

Discussions of the legal and political challenges and responsibilities of IoT regulation are almost exclusively found in social science journals, while journals on engineering and physical sciences focus on technical efforts to improve IoT security and privacy without necessarily acknowledging existing legislation. This is a finding by Veale et al., who wrote that "PbD, and the [Data Protection by Design] now mandated by law, is seen increasingly as a synonym for the formal privacy enhancing technologies literature that take reducing unwanted information disclosure as their sole goal," and advocated for more holistic perspectives on data protection principles (Veale, Binns, and Ausloos 2018).

Aside from academic literature, there are ample whitepapers written by corporations, such as vendors, and political organisations on the need for new regulatory standards. Some of these focused on the idea of IoT Security by Design, such as Australian "cyber agencies and industrial groups" in 2018 discussing designing much-needed IoT security controls without "constituting a coordinated strategy detailing how government and industry can collaborate on the IoT" (Chapman and Uren 2018). Another example is the 2014 UK government report that advocated for anticipatory regulation of emerging IoT technologies, which led to the 2024 IoT regulation law (Department for Digital, Culture, Media & Sport n.d.; Department for Science, Innovation and Technology, National Cyber Security Centre (NCSC) n.d.). Additionally, Rustad noted that the GDPR's "expansive extraterritorial effect" meant that it applies to IoT manufacturers outside the EU, provided that sales still occur to users within the affected countries. Rustad concluded that operationalising the GDPR's requirement of IoT PbD will be a challenge for manufacturers but that "the largest challenge" is "to safeguard the data they process, and to detect espionage and stave off cyberattacks [*sic*]" (Rustad 2019). This is a particularly relevant issue for journalists who may not be able to avoid interaction with the IoT but must nonetheless maintain source confidentiality and the integrity of their work.

Walker et al. surveyed the current state of both "hard" and "soft" laws that could be applicable to the IoT across several EU and US jurisdictions and noted a lack of "international coherence in IoT security policy" (Walker et al. 2018). This may result from varying degrees of input from the myriad of stakeholders, though they also found that there appeared to be cultural differences in terms of decision-makers' policy approaches to the IoT. They argue that policymakers in the US favoured solutions derived through consultation with industry while those in Europe instead chose to develop regulatory principles and guidelines to be subsequently imposed on industry.

In the US, Quirk noted that consumer IoT devices are largely the same electronics that have long been governed by the US Federal Communications Commission (FCC), just with added wireless modules (Kamalipour 2019; Quirk 2017). Thus manufacturers, importers and vendors must abide by ordained "specific technical standards, follow appropriate FCC equipment authorization procedures, and comply with quality practices." However, he did not mention regulation for the special purpose of heightening device security. Comparatively, Weber argued that a centralised regulatory body would be inappropriate in the US, however, he felt that there was a need for collaboration between state-affiliated entities for "democratic legitimacy", private sector and civil society partners to ensure that the IoT is both secure and confidential (Weber 2009).

Urquhart et al. stated that an aspect of regulation is accountability, so that parties involved in developing and creating multiple features of IoT devices (from potentially non-consensual data collection to inadequate user interfaces) are responsible for IoT performance to secure user trust (Urquhart, Lodge, and Crabtree 2019). Tusikov's book chapter recognised an oft overlooked facet of the regulatory discussion: ownership of devices (Tusikov 2019). This is relevant because the companies that develop and copyright proprietary IoT technologies, particularly software, retain a disproportionate amount of "post-purchase control" over devices through contractually agreed surveillance and user data collection capabilities. According to Mulligan, the rise of the IoT facilitated a shift in the contractual and licensing language used by these companies, from referring to customers as device "owners" to calling them "users", allowing the companies "downstream control" that is only legal because the devices contain chips rather than gears (Mulligan 2015). This indicated a lack of comprehension on the part of legislators and policymakers regarding digital devices and the contemporary manufacturer-customer relationship.

Evidently, the literature on legislation to address IoT threats is disparate and does not discuss the implications of insufficient regulation on journalists. This paper documents concerns raised by interviewees regarding the impact of inadequate government limitations on IoT threats to the media.

Methodology

This research establishes a snapshot of the impact of the IoT on press freedom considerations in four liberal democratic nation-states, primarily through 63 semi-structured interviews with journalists and relevant experts (George and Bennett 2005; Goodrick 2014; Kennett 2001; Mills, Durepos, and Wiebe 2010; Smets and Lievens 2018). Access to a pool of relevant professional contacts enabled purposive sampling of industry experts, threat intelligence experts and members of the media who have specialisms relevant to each country. Insight on these topics was gathered from summer 2020 through summer 2022 from a range of experts. Interviews were semi-structured and focused around particular themes that remain relevant in 2025 (Reporters without Borders n.d.a). This enabled detailed investigation of the similarities and differences between a small number of examples to develop theories that can guide policy (George and Bennett 2005).

There are anticipated challenges to mixed research methods case studies, such as potentially conflicting interview responses (Becker, Bryman, and Ferguson 2012). However, these problems were overcome with understanding of the environmental and experiential factors that affect participants. To reduce selection bias, approximately 280 experts were contacted and given information about the study (Bourgeault, Dingwall, and Vries 2010; Campbell et al. 2020). The participant pool was supplemented through snowball sampling, by asking interviewees to name other people who are experts in their niche, both who agree and disagree with them. All data has been protected according to UK law. By identifying any recurring responses and positions from the interviews and qualitative survey responses, themes were established that form the basis of this paper. This was done by transcribing interviews and long-form survey responses, before employing qualitative content analysis techniques adapted from

Erlingsson and Brysiewicz's five-step process (Barlett and Vavrus 2016; Erlingsson and Brysiewicz 2017).

Results and Discussion

This paper seeks to understand the extent to which existing laws and regulations in each of the case study countries facilitate risk from the IoT to the media. Interviewees overwhelmingly responded that laws and legislation that enable the acquisition of data from IoT devices by domestic government agencies is the most significant law-related IoT risk that they perceive to the media. This has been categorised under the theme "domestic government overreach.", and aligns with Reporters Without Borders 2024 World Press Freedom Index, finding that "a worrying decline in support and respect for media autonomy and an increase in pressure from the state or other political actors" is the indicator that has fallen the most in the last year, highlighting the continued relevance of this risk (Reporters without Borders n.d.a).

Within this theme, sections discuss legitimate interest carve-outs, journalistic and source data swept up in IoT surveillance, and mass surveillance and "Big Data". Then, this paper explores the second most frequently observed threat raised by interviewees, termed "domestic government inadequacy". Sections within this theme cover lacking legal protections against IoT threats and limited existing protections for journalistic work. These two themes are important findings to understand the lived realities of journalists and media organisations in four key countries. While geopolitical considerations such as supply chain risks formed a third significant theme arising from this study, length constraints mean that these are beyond the scope of this article.

Domestic Government Overreach

The most frequently mentioned IoT-related threat to the press that interviewees perceived was domestic government overreach through legal means: via state agencies using mechanisms in legislation to access data that could include information on journalists and their sources. Their fear was that this would enable surveillance, including pattern of life analysis, which could divulge source identities or unpublished story details to domestic state actors (Shere 2022). For example, logs from smart home devices like doorbell cameras and white goods can expose daily routines (Beyer et al. 2018), leaving journalists and their families vulnerable to physical attacks. Certain IoT devices including smartwatches and voice assistants can also reveal typing patterns (Christian 2015; Liverpool 2020) – this could allow the reconstruction of messages, allowing malicious actors to uncover investigative work and potentially use personal information for blackmail. Key reasons why interviewees reported fears about government are that there is an absence of information available as to countries' authorities' capabilities regarding the consumer IoT, and that laws and policies meant to protect the media from technological threats are insufficient.

Legitimate Interest Carve-Outs

Interviewees noted that one way in which states can access data and devices is through clauses in data protection legislation that purportedly limits access and transfer of data.

For instance, UK surveillance in the name of national security relating to counterterrorism and anti-foreign interference was named as often being sufficient justification to override pre-existing legal protections, including for journalists.[1] This includes Section 50 of the Regulation of Investigatory Powers Act 2000 (RIPA) which requires subjects to disclose "any key in his possession to obtain access to the information or to put it into an intelligible form" (Parliament of the United Kingdom 2000). This could include passwords to IoT devices, encryption keys or associated Cloud accounts and UK interviewees were concerned that refusal is punishable by a prison sentence.[2]

Similarly, US interviewees also recalled repeated attempts to legislate for minimal encryption in the name of national security, which would leave devices easily compromised and threaten the confidentiality of conversations between journalists and their sources and editors.[3] These include the government-mandated inbuilt backdoor in the encryption 1993 Clipper chip (Carney n.d.),[4] the EARN IT Act (2020)[5] and the 2020 Lawful Access to Encrypted Data Act (LAED Act), named by interviewees (Pfefferkorn 2020).[6] Further, P25, a Taiwanese lawyer with expertise in information technology, communications and telecoms, and technology law and policy, also said that the Taiwanese national security agencies have enough legal authority that they "don't need to go through the detailed and transparent, maybe judicial process before they directly collect the data from the companies."[7]

Research conducted to corroborate the issues raised by interviewees found that there are also carve-outs exempting over twenty Australian government agencies from compliance with the Privacy Act 1988, Australia's federal data protection framework (Australian Government n.d.). Although there was a 2023 Privacy Act 1988 Review and government response, it is unclear when changes to the Privacy Act 1988 will be made or precisely what they will be (Patto and Zhang 2023). As a result of these clauses in legislation that otherwise limits data access and control, domestic government agencies may be granted access to IoT devices and data associated with journalists. This could enable state agencies to identify sources, prevent the release of stories and tie journalists and media organisations up in lawsuits that drain their resources and hinder future reporting.

IoT Surveillance and Big Data

Interviewees considered surveillance laws that allow government access to data and devices via legal means to be less insidious and more common than legal carve-outs, but nevertheless overzealous means for domestic governments to threaten press freedom. This finding is relevant to IoT devices because their range of functionalities and the kinds of data that they can both collect and connect mean that journalists may be surveilled in new ways without governments needing to expand existing laws. Further, the prevalence of consumer IoT devices lowers the financial barrier for state agencies who might otherwise have had to invest in their own hardware, as now journalists may be monitored through their own devices and using the information they provide in private environments where there is the capacity for ambient surveillance.

Interviewees reiterated the substantial amount of national security and surveillance legislation that has been passed in the aftermath of 9/11 (Jones 2018). This was true in Australia,[8] which P42, a journalist of 30 years, recognised has "at least 82 [pieces of legislation], which is more than any other Western democracy." Further, four interviewees reported that Australia's cyber laws – which are a combination of state-level and territorial

laws that overlap with federal-level national security legislation regarding surveillance (DLA Piper: Law in Australia n.d.) – were seen as lacking when compared to European regulations;[9] asserting that this is likely to the benefit of the Australian government and the Five Eyes Intelligence network (Mann, Daly, and Molnar 2020; Wells 2020).[10] Four interviewees discussed that the speed of these kinds of laws being created made it difficult to raise concerns about them regarding press freedom (Parliament of Australia 2011; Parliament of Australia 2012; The Australian Privacy Foundation 2011).[11] Further, due to the interconnected nature of surveillance within alliances like Five Eyes, there is a risk that even if four member states have robust safeguards for journalism, those protections could be compromised to the point of being ineffective if the fifth state has weaker safeguards.

Interviewees commented on an element of legislation facilitating surveillance – the need, or lack thereof, for a warrant: in some countries, it is overwhelmingly difficult to challenge a warrant, and in other cases, there could be no legal requirement for a warrant to access media property and information. For instance, Australian interviewees recognised that challenging a warrant for access to journalistic material is hard because of inherent weakness in Australia's "implied" right of media freedom when compared to the legal legitimacy of a warrant.[12] For example, P42, a journalist of 30 years, argued that

> the warrant regime around (Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018) is incredibly lax, so the journalist's own data is exposed to police investigation and the relationship between journalists and their sources is exposed to police inquiry, and the sources themselves are becoming vulnerable to police prosecution.[13]

In fact, while agencies must obtain a Journalist Information Warrant (JIW) to access the metadata of journalists or their known or suspected sources, according to the Commonwealth Ombudsman, this safeguard has been bypassed multiple times since 2015 by police across Australia (Manthorpe 2021; Karp and Taylor n.d.).

Further, under the Australian Surveillance Legislation Amendment (Identify and Disrupt) Act 2021 (Home Affairs 2021), three new warrants were introduced that would apply to IoT devices ("data disruption warrants," "network activity warrants" and "account takeover warrants"). For journalists, these powers pose significant risks, as the definitions of "network" and "electronically linked" groups are broad, meaning surveillance could be conducted without knowing whether a journalist or their source is being targeted. This is particularly concerning for those working with confidential sources, including those overseas, who may inadvertently fall under surveillance (Mann and Murray 2021). Additionally, the law's low threshold for seriousness (covering offenses with sentences of three years or more) means journalists investigating government conduct or national security matters could be exposed to state hacking with tenuous justification (Harkin and Mann 2023). The weakness of safeguards around this Act may go well beyond exacerbating a chilling effect.

Similarly, the USA PATRIOT Act 2001 was described as "draconian" in its allowance of intrusive technical measures to enable access to data through hacking devices.[14] Additionally, the US's Electronic Communications and Privacy Act (1986) was noted by interviewees as only requiring a warrant to access digital content that is under 180 days old, and it may otherwise be accessed through a court order or administrative

subpoena. McGregor noted neither of these require "significant judicial oversight" to be granted, nor do data subjects need to be notified in a timely fashion (McGregor 2021).

Another feature of surveillance laws that interviewees found harrowing was the lack of confirmation as to whether surveillance was happening at all, preventing them from accurately assessing the risk to them and their sources (Daly, Robinson, and McMenemy 2022; Greenwald 2014). This uncertainty is exacerbated by the number and variety of ways in which the IoT can collect data (Shere, Nurse, and Martin 2023). US interviewees hoped that raising awareness of the types and quantities of data collected by the IoT would be sufficient to make government legal and policy responses more comprehensive.[15] However, self-censorship is a well-documented "chilling effect" consequence of laws enabling surveillance and the consequences of reporting against the interests of influential decision makers (Mills and Sarikakis 2016). For example, P4, an expert in state capabilities and legislation relating to use of IoT devices for surveillance of press in the UK, mentioned that in the UK, any suspected unlawful surveillance cases can be taken to the Investigatory Powers Tribunal (IPT), which operates under a "neither confirm nor deny" policy regarding whether the surveillance is happening at all.[16] Under the framework of the 2016 Investigatory Powers Act (IPA),[17] the Investigatory Powers Commissioner's Office (IPCO) must approve invasive powers such as surveillance warrants; however both a former Investigatory Powers Commissioner and the National Union of Journalists (NUJ) have argued that the powers granted by the IPA are too far-reaching, in the latter case as they include inadequate safeguards for confidential journalistic sources (Bowcott n.d.).

More concerns of these kinds were expressed in January 2024 by a variety of civil rights and technological interest groups in response to a proposed amendment to the IPA 2016 (The UK England Chapter of the Internet Society 2024; techUK n.d.). Despite these challenges, the Investigatory Powers (Amendment) Act passed into law in April 2024 (The Home Office 2024a; The Home Office 2024b). This Act expanded bulk data surveillance powers, facilitated by the creation of a category of bulk personal datasets where "the individuals to whom the personal data relates could have no, or only a low, reasonable expectation of privacy in relation to the data" (The Home Office 2024a). The Amendment Act includes an update to "journalistic safeguards", expanding on the conditions in which the powers may interact with confidential journalistic material and source information (The Home Office 2024a). The update explicitly states that with prior independent authorisation by the Investigatory Powers Commissioner, material obtained using bulk equipment interference may be searched with the "purpose" "to identify any confidential journalistic material or to identify or confirm a source of journalistic information" (The Home Office 2024a). As the IPA and its 2024 Amendment Act take a deliberately "technology-neutral approach" to surveillance and Big Data collection and analysis, these powers are intended to adapt to the "exceptional growth in the volume and type of data relating to people, objects, and locations" which the IoT offers, thereby representing a legal avenue for exploitation of IoT capabilities to affect media freedom (The Home Office 2024b). UK interviewees noted that, for journalists to trust safeguards in place through the IPT, they must rely on both judicial understanding of emerging technologies - ignoring the historic lack of technical knowledge - and on technical experts from the IPCO being sufficiently committed to press protections.[18]

The current state of legal surveillance was considered by interviewees to be indicative of a cultural norm of maximising intelligence gathering, resulting in collection and retention of Big Data (Casanovas et al. 2017). An extreme example of bulk data collection that was seen by interviewees as designed to enable government access is the Australian Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015.[19] This law compels telecoms companies to retain metadata associated with Australian citizens for at least two years. Research into interviewee concerns about this law found that it has been criticised for a number of reasons, including the fact that the legislation gives 22 government agencies access to the metadata without the need for a warrant,[20] and the telecoms companies have reported multiple instances of other agencies requesting illegal access to journalists' metadata (Karp and Taylor n.d.; Communications Alliance 2020). Although there is a provision in the law intended to protect press freedom by requiring a warrant before any retained data can be accessed by Australian state agencies for investigations focused on journalists, this still has the potential to "chill" journalistic expression, given the ubiquity of the IoT (Lashmar 2020).

Domestic Government Inadequacy

Domestic government inadequacy, manifesting in insufficient protections and regulations, was the second most frequently mentioned way in which domestic governments increase IoT risk for journalists. This is because it prevents journalists from being able to prioritise the IoT, relative to other drains on their time, energy and resources.

Insufficient Legal Protections against IoT Threats

One form of governmental inadequacy that enables IoT threats to the media is meagre regulation of the devices and data themselves. This received attention in 2023, showing a continued relevance since these interviews began in summer 2020, with attempts at motivating industry to self-regulate being concluded in favour of legislation such as the UK's Product Security and Telecommunications Infrastructure (PSTI) Act, which came into effect in April 2024 (Department for Science, Innovation and Technology, National Cyber Security Centre (NCSC) n.d.; Department for Digital, Culture, Media & Sport: Code of Practice for Consumer IoT Security 2018; Department for Digital, Culture, Media & Sport: Policy Paper: Government response to the call for views on consumer connected product cyber security legislation 2021; Department for Digital, Culture, Media & Sport n.d.; Department for Digital, Culture, Media & Sport, Warman MP, M. 2021; NCC Group 2021).[21] Likewise, the US has also attempted IoT regulation through legislation, as the Internet of Things Cybersecurity Improvement Act of 2020 compels the National Institute of Standards and Technology (NIST) to create "standards and guidelines" for IoT devices purchased and used by federal agencies (Kelly 2020). While the IoT Cybersecurity Improvement Act signals the US government's recognition that IoT threats could undermine democratic systems, these new regulations solely provide incentive for IoT manufacturers and vendors for federal systems, with some states making their own regulations (Stauss, Bowman, and Rogers n.d.). In March 2024, the US Federal Communications Commission (FCC) released a voluntary self-regulation "trust mark" scheme for consumer devices (Federal Communications Commission 2024). It is likely that the US is loath to forcibly regulate the consumer IoT market due to fears over stifling innovation. Taiwan

interviewees also noted that IoT regulation would be seen by the Taiwanese government as necessary to ensure fair market competition, rather than to increase device security for the sake of consumer protection.[22]

Another area of weakness in existing legislation that interviewees raised is unrealistic laws and regulations. For example, the 2018 California Consumer Privacy Act (CCPA) was noted by interviewees as being difficult both for companies to comply with and for consumers to understand and limited because of a lack of consistent enforcement.[23] Similarly, interviewees suggested that while the GDPR includes the right to data portability,[24] which means journalists should be able to access their personal data collected by a company in the IoT supply chain,[25] this is unrealistic due to the heterogeneity of the consumer IoT. They were concerned that, for example, two devices with the same label, e.g., both marketed as fitness trackers, might store their data so differently that effective collation or comparison of these datasets is unfeasible (Turner et al. 2021).[26] Literature corroborates such issues, such as Noto La Diega pointing out the difficulty of forcing IoT consumers to deal with challenges by wading through the "contractual quagmire" of overlapping legal documents pertaining to even one device, given the huge investment by UK decision-makers in IoT devices such as mandatory smart metres (Noto La Diega 2016). These consumers would include UK journalists and sources, complicating their efforts to minimise personal IoT risk.

Limited Existing Protections for Journalistic Work

Another key form of government inadequacy that was a source of concern for interviewees regarding all four countries is that established journalistic legal protections prove insufficient against government overreach and surveillance, including direct government and law enforcement interference. This has clearly continued, with multiple cases of these failures of journalistic safeguards reported from the UK, US and Australia in 2023–2024, but do not seem to have occurred in Taiwan, which moved up eight places in the 2024 World Press Freedom Index (International Federation of Journalists: Australia n.d.; Yu-fan and Lin 2024; McCormack 2024; Reporters without Borders: USA n.d.; Vogus 2024).

UK and US interviewees argued that source confidentiality and security are deteriorating despite the fact that the UK and the US have both significant journalistic protections against this kind of overreach: the First Amendment of the US Constitution and the UK's Bill of Rights.[27] They framed this within the context of the erosion of other democratic values due to changing norms in government enforcement that reduce pre-existing safeguards.[28] Taking this to an extreme, rather than a legislatively enshrined "right to free speech," interviewees noted that Australia has an "implied freedom of political communication," inferred from the Australian Constitution by the High Court during the 1997 Lange v Australian Broadcasting Corporation court case (High Court of Australia 1997; Rule of Law staff 2019).[29]

While there is no statutory regulation of journalism in either the UK or US, interviewees recognised norms and legislation that are intended to legally restrict press capabilities.[30] One example of informal press regulation in the UK that was named is the D-notice committee, which implements a UK-press-specific system intended to preserve national security (Greenslade 2015).[31] Interviewees described its purpose as nudging journalists to self-censor stories that could compromise military affairs, without creating public furore. Although the First Amendment provides protection for journalists in the US,[32]

interviewees were still concerned about legal threats to sources. They most often referenced the Espionage Act 1917, although they acknowledged that this has never been used to prosecute a mainstream news publisher but that it lacks a public interest defence and has been increasingly used against whistleblowers.[33]

In contrast, P5, who has 25 years of experience working on press freedom in Taiwan, posited that direct attacks on the media or press freedom in Taiwan "would be considered against Taiwanese values and would be noticed by the public."[34] While Taiwan's Personal Data Protection Act does not include any mention of the media, it was updated in 2023 to strengthen personal data rights, and a draft Whistleblower Protection Act ("Draft WPA") was submitted to the Legislative Yuan for deliberation in 2019 that allowed whistleblowers to be journalistic sources, together indicating national commitment to individual liberties (Global Legal Group n.d.; Preparatory Office of Personal Data Protection Commission n.d.). P5 instead framed Taiwan's challenges in this area as due to a "misunderstanding of 'press freedom' as a concept."[35] Interviewees argued that this misunderstanding stems from a history of martial law and Taiwan's proximity with China, leading to the Taiwanese government being afraid of restricting press freedom to such an extent that it under-regulates other threat factors and at the same time appears complacent regarding attacks on the media within Taiwan, because of their juxtaposition with China's treatment of journalists.[36] Analysis of interviewees responses found that this has resulted in a similar problem in Taiwan as in the other three countries: reporting on cyber security threats to journalists is low, despite ample media coverage of such threats to each country in general.[37]

In addition to the laws that threaten journalists' security via the IoT, interviewees mentioned other legal threats to media freedom that can be combined with carve-outs, surveillance laws and bulk data collection to compound the impacts on journalists of domestic government overreach. This includes legislation that UK interviewees believed impacts press freedom such as libel law,[38] which interviewees reported meant "anybody who had access to lawyers and funds could tie newspapers up for months, if not years in litigation over risk to reputation."[39] Interviewees feared that this drains financial resources, time and energy until the news organisation folds, sending a chilling message to the wider press. Interviewees noted a recent increase in "vexatious litigation" where claims are taken to UK courts in strategic lawsuits against public participation (known as SLAPP cases) that are intended to overwhelm and incapacitate sources of independent public interest journalism (Neate 2022).[40] British law firms and courts were noted by interviewees as often being chosen through "forum shopping" for a jurisdiction with laws that are preferential to claimants (Phillips 2020).[41] They gave the example of Appleby suing only the UK news organisations of the over 90 media partners involved in the Paradise Papers revelations for breach of confidence relating to the source materials (Guardian staff n.d.). P44, an expert in threats to press freedom in the UK and US, stated it

> felt very much like a test case […and…] the fact of that suit was concerning because it demonstrates that there's something about the UK's legal climate that makes it more attractive to take legal action against journalists here than in other jurisdictions.[42]

Conclusion

This article compared and contrasted the legal and policy challenges that increase IoT risk to the media industries and to journalists in Taiwan, Australia, the UK and the US. This

analysis enables an assessment of the extent to which existing laws and regulations in those countries facilitate risk from the IoT to the media. This research reveals persistent themes of technological threats to the media, exacerbated by increasingly inhospitable government attitudes toward the media (Reporters without Borders (RSF) n.d.b; Reporters without Borders n.d.b). Across the countries examined, interviewees highlighted the dearth of IoT-specific policy and legislation that regulates the security or privacy provisions of the consumer IoT or addresses the potential for serious threats enacted through adversarial use of these devices (DeNardis and Raymond 2017; Sicker 2019). This is primarily because of the recent and rapid development of the consumer IoT market, its fragmentation and poor privacy and security by design, and particularly the massive amounts of data collected by heterogeneous devices (Tusikov 2019). Interviewees expressed that this last factor is exacerbated by the high value placed upon intelligence by national governments, and a post-9/11 surveillance culture, which signal growing authoritarian tendencies even in democratic states and contribute to attacks on freedom of the press globally (Reporters without Borders (RSF) n.d.a; Reporters without Borders n.d.b).

This research demonstrates that the domestic confluence of technological, political and legal challenges exacerbates geopolitical concerns, creating challenging gaps in existing protection and mitigation methods used by journalists in democratic countries. In fact, techUK, the UK's technology trade association, wrote that the IPA Amendment Act 2024 "could become a model for less democratic governments" (Parliament of Australia 2011). Throughout, interviewees offered comparisons between the three Five Eyes countries analysed: as members of this intelligence network, they have similar priorities and histories regarding surveillance laws, which are relevant to the IoT and press freedom. It would therefore be relevant for future research to expand this interdisciplinary country profiling to Canada and New Zealand, to enable comparison between all Five Eyes partners. Additionally, further comparisons were drawn because Australia's legal procedures derive from the UK's (Kercher 2020), and Australia has a federal-state divide that impacts regulation akin to the US. This study showed the volume of relevant legislation passed in Australia to be perhaps the strongest example of domestic government overreach with the potential to exacerbate IoT risks to media freedom. However, the first month of the Trump Administration's second term saw a record number of Executive Orders, the reduction of established outlets' access to press briefings, and new political appointees whose rhetoric and actions have negative implications for media freedom in the US and globally (Reporters without Borders (RSF) n.d.b; Hamilton n.d.; Index on Censorship n.d.).

Myriad articles, legislation, and civil society reports published since these interviews were conducted demonstrate that this snapshot's themes of government overreach and inadequacy continue to intensify, and indicate that these findings are crucial for interpreting ongoing and likely future events. Fundamentally, this research underscores the vulnerability of journalists to new forms of surveillance and cyber-attacks, facilitated by the proliferation and advancement of IoT devices and regulatory frameworks that are insufficient to address convergence of emerging technologies (e.g., Artificial Intelligence) with IoT capabilities. Therefore, this study provides a valuable lens for understanding and addressing the intersection of technology, government action, and media freedom in the present and future.

Notes

1. Interviewee: P26
2. Interviewees: P4, P15
3. Interviewees: P59, P32
4. Interviewees: P51
5. Interviewee: P59
6. Interviewee: P34
7. Interviewees: P25, P29
8. Interviewees: P55, P42, P33
9. Interviewees: P28, P30, P33, P40
10. Interviewees: P28, P40, P15, P26, P44, P4
11. Interviewee: P55, P42, P56, P40
12. Interviewee: P42
13. Interviewee: P42
14. Interviewee: P41
15. Interviewee: P17
16. Interviewee: P4, P17
17. Interviewees: P4, P26, P44, P17, P43
18. Interviewee: P4
19. Interviewees: P40, P42, P28, P30, P33, P55, P36, P52
20. Interviewees: P42, P28, P52, P33, P55
21. Interviewees: P3, P14, P17, P18, P20, P27, P30, P31, P48, P50, P55, P60
22. Interviewees: P25, P49
23. Interviewee: P24
24. Interviewees: P17, P30
25. Interviewees: P31, P50
26. Interviewee: P50
27. Interviewees: P30, P55, P42, P27
28. Interviewees: P9, P44, P47, P23, P17, P4, P26, P43
29. Interviewees: P30, P42
30. Interviewees: P22, P23
31. Interviewees: P41, P4
32. Interviewees: P47, P23, P17
33. Interviewees: P9, P44, P47
34. Interviewee: P5
35. Interviewee: P5
36. Interviewees: P5, P49
37. Interviewees: P49, P5
38. Interviewees: P4, P22, P1, P53, P15, P44
39. Interviewee: P1
40. Interviewees: P15, P44
41. Interviewee: P44
42. Interviewee: P44

Acknowledgements

We thank all participants for generously offering their time and insights to ensure that this research is meaningful. We are additionally grateful to our reviewers for their kind words and help refining this work. Finally, thanks to Dr. Paul Lashmar for assessing the PhD from which this paper is derived, and recommending that we submit this material for publication!

Ethical Approval Details

The University of Oxford Central University Research Ethics Committee gave its approval for this study: approval number CS_C1A_20_003.

Disclosure Statement

This paper was researched/written before Dr. Shere was employed as a UK civil servant, and nothing herein is indicative of her current employer's perspective.

Funding

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

References

Australian Government: Australian Law Reform Commission. n.d. "The Number and Scope of Exemptions." Accessed August 16, 2010. https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/33-overview-exemptions-from-the-privacy-act/the-number-and-scope-of-exemptions/.

Ball, J. 2015. "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.

Barlett, L., and F. Vavrus. 2016. *Rethinking Case Study Research : A Comparative Approach*. New York: Routledge.

Becker, S., A. Bryman, and H. Ferguson, eds. 2012. *Understanding Research for Social Policy and Social Work*. Bristol: Policy Press.

Bentham, J. 2012. *The Works of Jeremy Bentham, vol. 4*. Edinburgh, Scotland: Online Library of Liberty.

Berger, G. 2018. "Is There a Future for Journalism?" *Journalism Practice* 12 (8): 939–953. https://doi.org/10.1080/17512786.2018.1516117.

Beyer, S. M., B. E. Mullins, S. R. Graham, and J. M. Bindewald. 2018. "Pattern-of-Life Modeling in Smart Homes." *IEEE Internet of Things Journal* 5:5317–5325. https://doi.org/10.1109/JIOT.2018.2840451.

Blythe, J. M., and S. D. Johnson. 2021. "A Systematic Review of Crime Facilitated by the Consumer Internet of Things." *Security Journal* 34(1): 97–125. https://doi.org/10.1057/s41284-019-00211-8.

Bourgeault, I., R. Dingwall, and R. de Vries. 2010. *The SAGE Handbook of Qualitative Methods in Health Research*. London, UK: SAGE Publications Ltd.

Bowcott, O. n.d. "'Bulk Hacking' by UK Spy Sgencies Is Illegal, High Court Told." Accessed May 17, 2019. http://www.theguardian.com/technology/2019/jun/17/liberty-mounts-latest-court-challenge-to-snoopers-charter-mi5-gchq.

Burgess, J., and E. Hurcombe. 2019. "Digital Journalism as Symptom, Response, and Agent of Change in the Platformed Media Environment." *Digital Journalism* 7 (3): 359–367. https://doi.org/10.1080/21670811.2018.1556313.

Campbell, S., M. Greenwood, S. Prior, T. Shearer, K. Walkem, S. Young, D. Bywaters, and K. Walker. 2020. "Purposive Sampling: Complex or Simple? Research Case Examples." *Journal of Research in Nursing* 25 (8): 652–661. https://doi.org/10.1177/1744987120927206.

Carney, D. n.d. "Summary: Security and Freedom through Encryption (SAFE) Act in 106th Congress." Accessed November 12, 1999. http://www.techlawjournal.com/cong106/encrypt/Default.htm.

Casanovas, P., L. De Koker, D. Mendelson, and D. Watts. 2017. "Regulation of Big Data: Perspectives on Strategy, Policy, law and Privacy." *Health and Technology* 7 (4): 335–349. https://doi.org/10.1007/s12553-017-0190-6.

Castro, D., and J. New. 2016. *Everything the U.S. Government Is Doing to Help the Private Sector Build the Internet of Things*. Washington, DC, USA: Center for Data Innovation.
Chapman, E., and T. Uren. 2018. *The Internet of Insecure Things*. Canberra, Australia: Australian Strategic Policy Institute.
Christian, J. 2015. "Here's How Your Smartwatch Can Reveal What You're Typing." https://www.vice.com/en/article/heres-how-your-smartphone-can-reveal-what-youre-typing/.
Clarke, R. 1988. "Information Technology and Dataveillance." *Communications of the ACM* 31 (5): 498–512. https://doi.org/10.1145/42411.42413.
Communications Alliance: Government Must Support Security Committee Recommendations and Repair the Data Retention Regime. 2020. "Communications Alliance, Sydney, Australia.".
Daly, A., E. Robinson, and D. McMenemy. 2022. *Cyber Security, Surveillance and Journalism in Scotland*. Dundee, Scotland: University of Dundee.
Day, M., G. Turner, and N. Drozdiak. 2019. "Amazon Workers Are Listening to What You Tell Alexa." https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio.
DeNardis, L., and M. Raymond. 2017. "The Internet of Things as a Global Policy Frontier." *UC Davis Law Review* 51 (23): 475–497.
Department for Digital, Culture, Media & Sport: Code of Practice for Consumer IoT Security. 2018. "Department for Digital, Culture, Media & Sport, London, UK.".
Department for Digital, Culture, Media & Sport. n.d. "Government response to the Regulatory proposals for consumer Internet of Things (IoT) security consultation." Accessed January 27, 2020. https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security/outcome/government-response-to-the-regulatory-proposals-for-consumer-internet-of-things-iot-security-consultation.
Department for Digital, Culture, Media & Sport: Policy Paper: Government response to the call for views on consumer connected product cyber security legislation. 2021. "Department for Digital, Culture, Media & Sport, London.".
Department for Digital, Culture, Media & Sport: The Product Security and Telecommunications Infrastructure (PSTI). n.d. "Bill – Product Security Factsheet." Accessed December 1, 2021. https://www.gov.uk/guidance/the-product-security-and-telecommunications-infrastructure-psti-bill-product-security-factsheet.
Department for Digital, Culture, Media & Sport, Warman MP, M. 2021. "Press release: New cyber security laws to protect smart devices amid pandemic sales surge." https://www.gov.uk/government/news/new-cyber-security-laws-to-protect-smart-devices-amid-pandemic-sales-surge.
Department of Home Affairs: Voluntary Code of Practice: Securing the Internet of Things for Consumers. n.d. Accessed September 2, 2020. https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/code-of-practice.
Department of Investment Service, Ministry of Economic Affairs: Key Industries: The Internet of Things. n.d. Accessed September 30, 2019. https://www.contacttaiwan.tw/.
Di Salvo, P. 2022. ""We Have to Act Like Our Devices Are Already Infected": Investigative Journalists and Internet Surveillance." *Journalism Practice* 16:1849–1866. https://doi.org/10.1080/17512786.2021.2014346.
DLA Piper: Law in Australia. n.d. Accessed January 28, 2019. https://www.dlapiperdataprotection.com/index.html?t=law&c=AU&c2=.
DLA Piper: Law in Taiwan, China. n.d. Accessed January 28, 2019. https://www.dlapiperdataprotection.com/index.html?t=law&c=TW.
DLA Piper: Law in United States. n.d. Accessed January 28, 2019. https://www.dlapiperdataprotection.com/index.html?t=law&c=US&c2=.
Erlingsson, C., and P. Brysiewicz. 2017. "A Hands-on Guide to Doing Content Analysis." *African Journal of Emergency Medicine* 7 (3): 93–99. https://doi.org/10.1016/j.afjem.2017.08.001.
Federal Communications Commission: FCC Adopts Rules for IoT Cybersecurity Labeling Program. 2024. "Public Safety and Homeland Security, Washington, D.C.".

Galič, M., T. Timan, and B.-J. Koops. 2017. ": Bentham, Deleuze and beyond: An Overview of Surveillance Theories from the Panopticon to Participation." *Philosophy & Technology* 30 (1): 9–37. https://doi.org/10.1007/s13347-016-0219-1.

George, A.L., Bennett, A. 2005. *Case Studies and Theory Development in the Social Sciences*. Cambridge, MA: MIT Press.

Global Legal Group: International Comparative Legal Guides. n.d. "Data Protection Laws and Regulations Taiwan 2023-2024." Accessed July 20, 2023. https://iclg.com/practice-areas/data-protection-laws-and-regulations/taiwan.

Goodrick, D. 2014. *Comparative Case Studies: Methodological Briefs – Impact Evaluation No. 9*. Florence, Italy: UNICEF-IRC.

Greenslade, R. 2015. "The D-Notice System: A Typically British Fudge That Has Survived a Century." http://www.theguardian.com/media/2015/jul/31/d-notice-system-state-media-press-freedom.

Greenwald, G. 2014. *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. Henry Holt and Company, New York, NY, USA: Metropolitan Books.

Guardian staff: Paradise Papers legal action against BBC and Guardian condemned. n.d. Accessed December 19, 2017. http://www.theguardian.com/uk-news/2017/dec/19/paradise-papers-legal-action-against-bbc-and-guardian-condemned.

Gunashekar, S., A. Spisak, K. Dean, N. Ryan, L. Lepetit, and P. Cornish. 2016. *Accelerating the Internet of Things in the UK: Using Policy to Support Practice*. Santa Monica, CA: RAND Corporation.

Haggerty, K. D., and Richard V. Ericson. 2000. "The Surveillant Assemblage." *British Journal of Sociology* 51 (4): 605–622. https://doi.org/10.1080/00071310020015280.

Hamilton, R. n.d. "Connecting the Dots: Trump's Tightening Grip on Press Freedom." Accessed February 6, 2025. https://www.justsecurity.org/107377/trump-control-us-media-information/.

Harkin, D., and M. Mann. 2023. "Electronic Surveillance and Australian Journalism: Surveillance Normalization and Emergent *Norms of Information Security*." *Digital Journalism*, 1–20. https://doi.org/10.1080/21670811.2023.2220366.

High Court of Australia: Lange v Australian Broadcasting Corporation ('Political Free Speech case'). 1997.

Home Affairs: Surveillance Legislation Amendment (Identify and Disrupt) Act 2021. 2021.

Index on Censorship: How Might Donald Trump's executive orders impact free speech? n.d. Accessed January 22, 2025. https://www.indexoncensorship.org/2025/01/how-might-donald-trumps-executive-orders-impact-free-speech/.

Information Commissioner's Office: Data Protection Act. 2018. "For Organisations." https://ico.org.uk/for-organisations/data-protection-act-2018/.

International Federation of Journalists: Australia. n.d. "ABC Faces Legal Threats over Climate Activism Footage / IFJ." Accessed October 12, 2023. https://www.ifj.org/media-centre/news/detail/category/press-releases/article/australia-abc-faces-legal-threats-over-climate-activism-footage.

Jones, D. M. 2018. "Intelligence and the Management of National Security: The Post 9/11 Evolution of an Australian National Security Community." *Intelligence and National Security* 33 (1): 1–20. https://doi.org/10.1080/02684527.2016.1259796.

Kamalipour, Y. R., ed. 2019. *Global Communication: A Multicultural Perspective*. Lanham, MD: Rowman & Littlefield Publishers.

Karp, P., and J. Taylor. n.d. "Police Made Illegal Metadata Searches and Obtained Invalid Warrants Targeting Journalists." Accessed July 23, 2019. http://www.theguardian.com/australia-news/2019/jul/23/police-made-illegal-metadata-searches-and-obtained-invalid-warrants-targeting-journalists.

Kazansky, B., and S. Milan. 2021. ""Bodies Not Templates": Contesting Dominant Algorithmic Imaginaries." *New Media & Society* 23 (2): 363–381. https://doi.org/10.1177/1461444820929316.

Kelly, R. L.. 2020. "Text - H.R.1668 - 116th Congress (2019-2020): IoT Cybersecurity Improvement Act of 2020.".

Kennett, P. 2001. *Comparative Social Policy: Theory and Research*. Buckingham; Philadelphia: Open University Press.

Kenyon, M. 2019. "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/.
Kercher, B. 2020. *An Unruly Child: A History of law in Australia*. New York, NY, USA: Routledge.
Lashmar, P. 2017. "No More Sources?" *Journalism Practice* 11 (6): 665–688. https://doi.org/10.1080/17512786.2016.1179587.
Lashmar, P. 2020. *Spies, Spin and the Fourth Estate: British Intelligence and the Media*. Edinburgh, Scotland: Edinburgh University Press.
Liverpool, L. 2020. "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/.
Department for Science, Innovation and Technology, National Cyber Security Centre (NCSC), Office for Product Safety and Standards, Lopez, J., n.d. "Viscount Camrose: New Laws to Protect Consumers from Cyber Criminals Come into Force in the UK." Accessed April 29, 2024. https://www.gov.uk/government/news/new-laws-to-protect-consumers-from-cyber-criminals-come-into-force-in-the-uk.
Lyon, D. 2018. *The Culture of Surveillance: Watching as a Way of Life*. Cambridge, UK: Polity Press.
Mann, M., A. Daly, and A. Molnar. 2020. "Regulatory Arbitrage and Transnational Surveillance: Australia's Extraterritorial Assistance to Access Encrypted Communications." *Internet Policy Review* 9: 1–20.
Mann, M., and A. Murray. 2021. "Striking a Balance: Legislative Expansions for Electronic Communications Surveillance." *Precedent (Sydney, N.S.W.)*. (166): 44–51. https://doi.org/10.3316/informit.118537295580986.
Mann, S. 2016. "Surveillance (Oversight), Sousveillance (Undersight), and Metaveillance (Seeing Sight Itself)." In *2016 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, 1408–1417. Las Vegas, NV, USA: IEEE Computer Society. https://doi.org/10.1109/CVPRW.2016.177.
Manthorpe, M. 2021. *Australian Federal Police's (AFP) Use and Administration of Telecommunications Data Powers 2010 to 2020*. Canberra, Australia: Commonwealth Ombudsman.
McCormack, J. 2024. "Naomi Long holds off on inquiry into police spying allegations." https://www.bbc.com/news/articles/cevvyvndlz5o.
McGregor, S. E. 2021. *Information Security Essentials*. New York, NY, USA: Columbia University Press.
Mills, A., G. Durepos, and E. Wiebe2010. "Comparative Case Study." In *Encyclopedia of Case Study Research*, 175–176. Thousand Oaks California, United States: SAGE Publications, Inc. https://doi.org/10.4135/9781412957397.n64.
Mills, A., and K. Sarikakis. 2016. "Reluctant Activists? The Impact of Legislative and Structural Attempts of Surveillance on Investigative Journalism." *Big Data & Society* 3 (2): 2053951716669381. https://doi.org/10.1177/2053951716669381.
Mulligan, C. 2015. "Personal Property Servitudes on the Internet of Things." *Georgia Law Review* 50:1121–1168.
NCC Group: UK government announces plans for new IoT security law. 2021. https://newsroom.nccgroup.com/news/uk-government-announces-plans-for-new-iot-security-law-425797.
Neate, R., Correspondent, R.N.W. 2022. "Senior Media Figures Call for Law to Stop Oligarchs Silencing UK Journalists." https://www.theguardian.com/news/2022/nov/29/slapps-senior-media-figures-call-for-law-stop-oligarchs-silencing-uk-journalists.
Noto La Diega, G. 2016. "Clouds of Things: Data Protection and Consumer Law at the Intersection of Cloud Computing and the Internet of Things in the United Kingdom." *Journal of Law & Economic Regulation* 9:69–93.
Nurse, J., A. Erola, I. Agrafiotis, M. Goldsmith, and S. Creese. 2015. "Smart Insiders: Exploring the Threat from Insiders Using the Internet-of-Things." Proceedings of the 2015 International Workshop on Secure Internet of Things (SIoT), Vienna, Austria.
Parliament of Australia: Cybercrime Legislation Amendment Act 2012. 2012. "Attorney-General's Department.".
Parliament of Australia: Cybercrime Legislation Amendment Bill 2011. 2011.

Parliament of the United Kingdom: Regulation of Investigatory Powers Act 2000. 2000. "Part III: Power to Require Disclosure: Section 50: Effect of Notice Imposing Disclosure Requirement." Statute Law Database.

Patto, J., and A. Zhang. 2023. "Government Response to the Privacy Act Review Report." https://www.pwc.com.au/legal/publications/2023-Government-Response-to-the-Privacy-Act-Review-Report.html.

Pfefferkorn, R. 2020. "There's Now an Even Worse Anti-encryption Bill Than EARN IT. That Doesn't Make the EARN IT Bill OK." https://cyberlaw.stanford.edu/blog/2020/06/there%E2%80%99s-now-even-worse-anti-encryption-bill-earn-it-doesn%E2%80%99t-make-earn-it-bill-ok.

Phillips, G. 2020. "How the Free Press Worldwide Is under Threat." https://www.theguardian.com/media/2020/may/28/how-the-free-press-worldwide-is-under-threat.

Preparatory Office of Personal Data Protection Commission (個人資料保護委員會籌備處). n.d. "Personal Data Protection Act." Accessed May 31, 2023. https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=I0050021.

Quirk, R. E. 2017. "Are Your Company's Consumer Electronics Exempt from FCC Marketing Regulations? [Future Directions]." *IEEE Consumer Electronics Magazine* 6:22–26. https://doi.org/10.1109/MCE.2016.2640578.

Reporters without Borders (RSF). n.d.a "2024 World Press Freedom Index – journalism under political pressure | RSF." https://rsf.org/en/2024-world-press-freedom-index-journalism-under-political-pressure.

Reporters without Borders (RSF). n.d.b "Only nine percent of humankind lives in a country Where press freedom Is good." Accessed May 2, 2019. https://rsf.org/en/news/only-nine-percent-humankind-lives-country-where-press-freedom-good.

Reporters without Borders (RSF). n.d.a "#SPOILERSFORFREEDOM: Exiled journalists warn democracies about decline in media freedom." Accessed April 27, 2017. https://rsf.org/en/news/spoilersforfreedom-exiled-journalists-warn-democracies-about-decline-media-freedom.

Reporters without Borders (RSF). n.d.b "One month of Trump: Press freedom under siege | RSF." Accessed February 19, 2025. https://rsf.org/en/one-month-trump-press-freedom-under-siege.

Reporters without Borders (RSF): USA. n.d. "Police Must respect rights of journalists to cover protests | RSF." Accessed May 3, 2024. https://rsf.org/en/usa-police-must-respect-rights-journalists-cover-protests.

Rule of Law staff: Implied Freedom of Political Communication - Case Note and New Resource. 2019. https://www.ruleoflaw.org.au/implied-freedom-of-political-communication-case-note-and-new-resource/.

Russell, A., R. Kunelius, H. Heikkilä, and D. Yagodin, eds. 2017. *Journalism and the NSA Revelations: Privacy, Security and the Press. I.B. Tauris Ltd in Association with the Reuters Institute for the Study of Journalism*. Oxford, UK: University of Oxford.

Rustad, M. L. 2019. "How the EU's General Data Protection Regulation Will Protect Consumers Using Smart Devices." *Suffolk U. L. Rev* 52:227–272.

Shere, A. 2021. "How the Internet of Things Poses a Threat to Journalists." https://journalistsresource.org/home/how-the-internet-of-things-poses-a-threat-to-journalists/.

Shere, A. R. K., J. R. C. Nurse, and A. P. Martin. 2023. "Threats to Journalists from the Consumer Internet of Things." In *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media*. Springer Proceedings in Complexity, edited by C. Onwubiko, et al., 303–326. Wales, UK: Springer. https://doi.org/10.1007/978-981-19-6414-5_17.

Shere, A. R. K. 2022. "6 Ways the Internet of Things Poses Security Threats to Journalists." https://journalistsresource.org/media/6-ways-the-internet-of-things-poses-security-threats-to-journalists/.

Shere, A. R. K., J. R. C. Nurse, and I. Flechais. 2020. "'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.

Sicker, D. C. 2019. "The Breadth of Policy and Regulatory Issues Facing IoT." *IEEE Internet of Things Magazine* 2:4–5. https://doi.org/10.1109/MIOT.2019.8835416.

Smets, A., and B. Lievens. 2018. "Human Sensemaking in the Smart City: A Research Approach Merging Big and Thick Data." *Ethnographic Praxis in Industry Conference Proceedings* 2018 (1): 179–194. https://doi.org/10.1111/1559-8918.2018.01203.

Srivastava, M., J. Shotter, C. Clover, R. Jalabi, and C. Cornish. 2024. "How Israeli Spies Penetrated Hizbollah." https://www.ft.com/content/6638813e-e246-4409-9a38-95bf60a220a8.

Stauss, D., B. Bowman, and M. Rogers. n.d. "Two New State IoT Laws Go into Effect on January 1." Accessed October 27, 2019. https://www.bytebacklaw.com/2019/10/two-new-state-iot-laws-go-into-effect-on-january-1/.

techUK: As the Government reviews the Investigatory Powers Act's notices regime. n.d. "It Is Vital We Maintain Proper Checks and Balances to Protect Privacy." Accessed August 10, 2023. https://www.techuk.org/resource/as-the-government-reviews-the-investigatory-powers-act-s-notices-regime-it-is-vital-we-maintain-proper-checks-and-balances-to-protect-privacy.html.

The Australian Privacy Foundation: The Cybercrime Bill Is Excessive and Unbalanced. 2011. "The Australian Privacy Foundation.".

The Home Office: Investigatory Powers (Amendment) Act 2024. 2024. "Statute Law Database.".

The Home Office: Investigatory Powers (Amendment) Bill 2023: Impact Assessment. 2024. "The Home Office, Whitehall, London, UK.".

The UK England Chapter of the Internet Society: Joint Briefing on Investigatory Powers. 2024. "(Amendment) Bill [HL]." https://isoc-e.org/joint-briefing-on-ipab-hl/.

Thompson, L. n.d. "Why Taiwan Has Become The 'Geographical Pivot of History' in the Pacific Age." Accessed September 29, 2020. https://www.forbes.com/sites/lorenthompson/2020/09/29/why-taiwan-has-become-the-geographical-pivot-of-history-in-the-pacific-age/.

Tian, S., L. Liu, and C. Y. Christian. 2004. "Course-Specific Corpora in the Classroom: A News Media English Class in Taiwan." *The Journal of Asia TEFL* 1:267–290.

Turner, S., J. Galindo Quintero, S. Turner, J. Lis, and L. M. Tanczer. 2021. "The Exercisability of the Right to Data Portability in the Emerging Internet of Things (IoT) Environment." *New Media & Society* 23(10): 2861–2881. https://doi.org/10.1177/1461444820934033.

Tusikov, N. 2019. "Precarious Ownership of the Internet of Things in the Age of Data." In *Information, Technology and Control in a Changing World: Understanding Power Structures in the 21st Century*, edited by B. Haggart, K. Henne, and N. Tusikov, 121–148. Cham: Springer International Publishing.

UNESCO. 2015. "Reporters without Borders: SAFETY GUIDE FOR JOURNALISTS: A Handbook for Reporters in High-Risk Environments." Reporters without borders.

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

Veale, M., R. D. P. Binns, and J. Ausloos. 2018. "When Data Protection by Design and Data Subject Rights Clash." *International Data Privacy Law* 8 (2): 105–123. https://doi.org/10.1093/idpl/ipy002.

Vogus, C. 2024. "Police Are Still Arresting Journalists." Why?, https://freedom.press/news/police-are-still-arresting-journalists-why/.

Walker, M., K. Shockey, A. Neiman, and A. Stephan. 2018. "Awakening Global Governments: An International Survey of Internet of Things Regulation." In *TPRC 46: The 46th Research Conference on Communication, Information and Internet Policy 2018*. Rochester, NY: Social Science Research Network. https://doi.org/10.2139/ssrn.3142105.

Weber, R. H. 2009. "Internet of Things – Need for a New Legal Environment?" *Computer Law & Security Review* 25 (6): 522–527. https://doi.org/10.1016/j.clsr.2009.09.002.

Wells, A.R. 2020. *Between Five Eyes: 50 Years of Intelligence Sharing*. UK, Casemate: Casemate.

Yu-fan, T., and K. Lin. 2024. "Taiwan Ranked 27th in 2024 RSF Press Freedom Index - Focus Taiwan." https://focustaiwan.tw/politics/202405030018.

Zuboff, S. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books Ltd.