The UK Code of Practice for Consumer IoT Security

Where we are and what next

Saheli Datta Burton

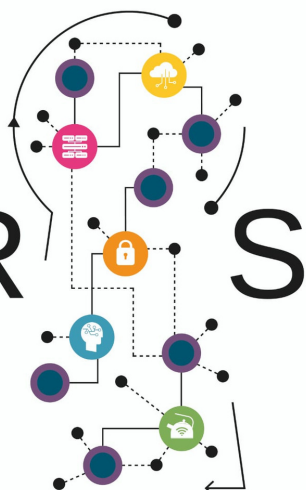**Leonie Maria Tanczer**

Srinidhi Vasudevan

Stephen Hailes

Madeline Carr

Department of Science, Technology, Engineering, and Public Policy (STEaPP)
University College London

PETR S

THE PETRAS NATIONAL
CENTRE OF EXCELLENCE
FOR IoT SYSTEMS
CYBERSECURITY

About this report

This report has been produced by the *Geopolitics of Industrial Internet of Things Standards* (GISt) research project led by Professors Madeline Carr and Stephen Hailes, and the *Building Evidence for CoP Legislation* (BECL) research project led by Dr Saheli Datta Burton and commisioned by the Secure-by-Design team of the United Kingdom Department of Digital, Culture, Media and Sport (DCMS).

Both GISt and BECL projects are held at the Department of Science, Technology, Engineering and Public Policy (STEaPP), University College London and funded by The PETRAS National Centre of Excellence for IoT Systems Cybersecurity, a consortium of leading UK universities dedicated to understanding critical issues in the privacy, ethics, trust, reliability, acceptability, and security of the Internet of Things. Funding for PETRAS is provided by the UKRI's Strategic Priorities Fund as part of the Security of Digital Technologies at the Periphery (SDTaP) programme.

▲UCL

DEPARTMENT OF SCIENCE, TECHNOLOGY, ENGINEERING AND PUBLIC POLICY

Authors

Saheli Datta Burton is a Research Fellow at the Department of Science, Technology, Engineering and Public Policy (STEaPP), University College London. She is the Principal Investigator for the EPSRC funded PETRAS project *Building Evidence for Code of Practice Legislation* (BECL), a Visiting Research Fellow at the Department of Politics, University of Vienna; Newton Fellow, Indian Institute of Science, India; Editor of Science & Technology Studies, journal of the European Association for the Study of Science and Technology (EASST) and former Research Associate at the Department of Global Health and Social Medicine, King's College London. Saheli holds an PhD and MSc from the Faculty of Social Science and Public Policy at King's College London and a BA in Economics from Columbia University, USA. Saheli is interested in the international political economy of emerging digital technologies with a focus on health and medicine.

Leonie Maria Tanczer is a Lecturer in International Security and Emerging Technologies at University College London's (UCL) Department of Science, Technology, Engineering and Public Policy (STEaPP). She is member of the Advisory Council of the Open Rights Group (ORG), affiliated with UCL's Academic Centre of Excellence in Cyber Security Research (ACE-CSR), and former Fellow at the Alexander von Humboldt Institute for Internet and Society (HIIG) in Berlin. Prior to her lectureship appointment, Tanczer was Postdoctoral Research Associate for the EPSRC-funded PETRAS Internet of Things (IoT) Research Hub, where she was part of its "Standards, Governance and Policy" research team. Tanczer holds a PhD from the School of History, Anthropology, Philosophy and Politics (HAPP) at Queen's University Belfast (QUB). Her interdisciplinary PhD project included supervision from both social sciences and engineering (ECIT) and focused on the (in)securitisation of hacking and hacktivism. She studied Political Science (B.A.) at the University of Vienna and University of Limerick (Republic of Ireland) and Political Psychology (MSc.) at Queen's University Belfast.

Srinidhi Vasudevan is a Research Fellow at the department of Science, Technology, Engineering and Public Policy (STEaPP), University College London. She is the Co-Investigator for the EPSRC funded PETRAS project Building Evidence for Code of Practice Legislation (BECL), and a visiting fellow at the Centre for Business Network Analysis (CBNA), University of Greenwich. Srinidhi holds a PhD from the University of Greenwich where her interdisciplinary work focused on interorganisational networks and financial decisions of listed firms. She holds a master's degree in information security from Royal Holloway, University of London and a bachelor's degree in computer applications from University of Madras. She specialises in data-driven modelling of risk behaviour using a network approach. Her current work focuses on board engagement pertaining to cybersecurity.

Authors (cont)

Stephen Hailes is the UCL Computer Science Head of Department and previously served as Professor of Wireless Systems and Deputy Head of UCL Computer Science. Stephen's research interests have three main directions: trust and security, in which he was one of the founders of the field of computational trust; networking, in which he has contributed to the development of the next generation Internet and to the security of networked industrial control systems; and mobile, robotic and sensor systems. Professor Hailes has attracted considerable funding, and has built a set of interdisciplinary relationships in seeking to address challenging problems in the real world. He has contributed to over 300 scientific papers, published in journals and conferences in AI, Machine Learning, Robotics and Automation, Behavioural Ecology and Sociology, Information Security and Computer Networking.

Madeline Carr is the Professor of Global Politics and Cyber Security in the Department of Science, Technology, Engineering and Public Policy, University College London. She is Director of the UK-wide Research Institute for Sociotechnical Cyber Security (RISCS) which looks at the human and organisational factors of cybersecurity. She is also the Director of the Digital Technologies Policy Lab which supports policy making to adapt to the pace of change in society's integration of digital technologies. Her research focuses on the implications of emerging technology for national and global security, international order and global governance. Professor Carr has published on cyber norms, multi-stakeholder Internet governance, the future of the insurance sector in the IoT, cybersecurity and international law, and the public/private partnership in national cyber security strategies. Professor Carr was the Co-lead on the Standards, Governance and Policy stream of the UK's £24M PETRAS research hub on the cyber security of the Internet of Things and now works on the international strategy for the National Centre of Excellence. Professor Carr is a member of the World Economic Forum Global Council on the IoT.

Contact:

saheli.burton@ucl.ac.uk

l.tanczer@ucl.ac.uk

s.vasudevan@ucl.ac.uk

s.hailes@cs.ucl.ac.uk

m.carr@ucl.ac.uk

Acknowledgements

Executive Summary

The Internet of Things (IoT) is emerging quickly in a range of consumer markets from toys to fitness (or wellness) devices to household appliances. These hold great promise for enhancing people's lives, improving our health and well-being, and streamlining or automating a range of daily functions. They also, however, introduce a range of risks including external manipulation, data breaches, surveillance, and physical harm. While consumer devices are often subject to regulation, standards or codes, these have not previously incorporated the new challenges and risks that arise in IoT consumer devices.

The UK has been proactive in considering how current regulatory frameworks, best practices, guidance, and other resources can support the uptake of innovations in consumer IoT devices in a safe and secure way. Through the PETRAS Cybersecurity of the Internet of Things research hub – now the National Centre of Excellence for IoT Systems Cybersecurity, we have worked to support DCMS to develop the Code of Practice for IoT Security (CoP). Seeing this work, alongside the significant contributions from multiple stakeholders, including industry, governments and civil society, contribute to the development of an ETSI Standard was exciting and a real demonstration of the value of interdisciplinary academic teams working closely with industry and policy makers to bring about positive change.

This work is not complete though. Adapting the standards, governance and policy of emerging technologies is an iterative process that requires constant reflection, evaluation, analysis and reconsideration as both the implementations develop and as our use (or misuse) of them evolves.

This report picks out **three issues** that we feel require urgent consideration.

- The **use of IoT devices by perpetrators of domestic abuse** is a pressing and deeply concerning problem that is largely hidden from view. Collecting data (and therefore evidence) on this is challenging for a number of reasons outlined in this section by Leonie Tanczer. There are concrete steps that both industry and the policy community could take to address the misuse of consumer IoT in this setting and we include a number of these as well as lessons from other countries.

- **Fitness devices** are also raising concerns as they have proven easy to compromise and they reveal deeply personal information about people's bodies, their homes and their movements. While IoT medical devices are regulated, there is a grey zone between these and fitness devices that results in a regulatory gap. Saheli Datta Burton has compared these two classes of devices, the ways they are vulnerable, the ways they are used, and the steps that could further secure fitness devices for the consumer market.

- Finally, **children's IoT connected toys** are coming under necessary scrutiny due to the implications of embedded cameras and microphones for a child's (or parent's) protection and right to privacy. These connected toys have the potential for misuse and unauthorised contact with vulnerable minors. The British Toy and Hobby Association has responded to this by offering a range of guidance notes and by interpreting the CoP but with SMEs making up the bulk of IoCT manufacturing, there is plenty more to be done to ensure that these organisations are sufficiently informed and equipped to avoid producing and marketing insecure toys.

This report highlights how a weak supply-side commitment to basic cybersecurity requirements in IoT manufacturing such as inbuilt encryption, password protection before distribution, user authentication (e.g., multi-factor authentication), regular audits and assessments exacerbates the plight of domestic 'tech abuse' victims, users of fitness devices, children, and their families. A complexity of shared technological, socio-ethical, regulatory and economic imperatives with some sector-specific nuances are at the heart of low-security manufacturing across sectors.

In addition to this work, our report also provides insight into **how widely the UK CoP has spread** since its publication in March 2018, especially its rapid development (with significant contributions of various stakeholders including industry, governments and civil society) to a technical specification (TS 103 645 in February 2019) and, recently, the ETSI EN 303 645 in June 2020. While these developments might be expected to lead to widespread adoption of related secure manufacturing practices in the EU, the infographics we provide demonstrate how widely the standards are being discussed and taken up. Tracking this is, in itself, a useful exercise as it allow us to better understand how technical standards are socialised through diverse stakeholder groups.

This report is certainly not the final word on the intersection between consumer IoT and policy responses. Nor will this be the last time we return to this work. But it is an update on where we are now and where we feel we need to be heading. Developing effective policies, regulations, standards, and guidance to protect citizens and to support service providers and manufacturers in the IoT is a challenging task that calls for input from many quarters. We are delighted that we have been able to make this contribution through PETRAS and sincerely thank all of those who have read and provided feedback on it.

Co-occurence network analysis revealed 2279 unique websites that mentioned the keywords and 10,000 unique matches with keywords within the 2279 websites (see Annex 1)
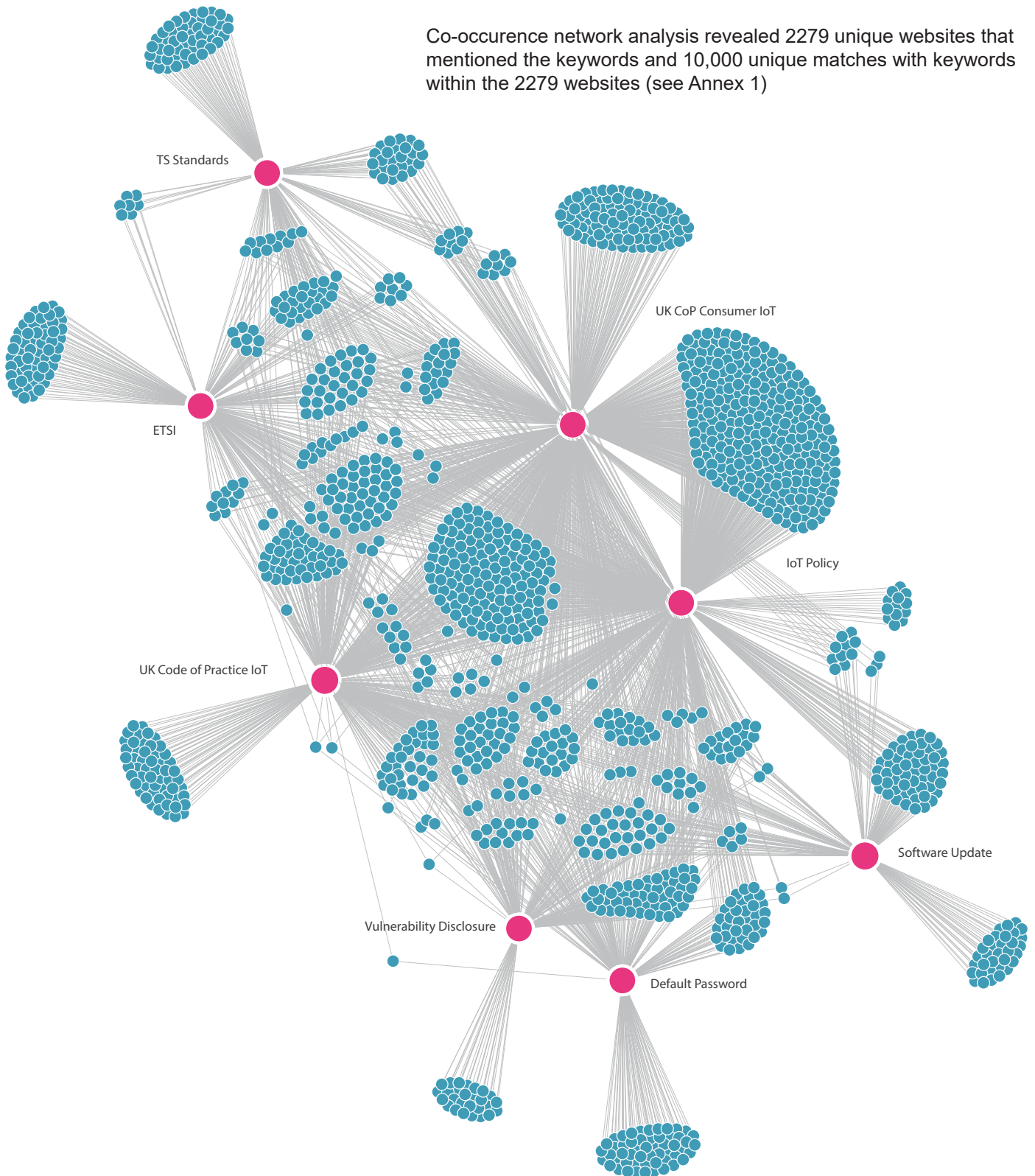
These keywords (pink dots) were searched to better understand the global uptake of the UK CoP and revealed 2279 unique websites (blue dots). Each of the 10,000 silver lines on this diagram represents a unique instance of the keyword mentioned within those websites. For more on this, please read Section 2.

Table of Contents

List of Figures

Introduction

The Internet of Things (IoT) is emerging quickly in a range of consumer markets from toys to fitness (or wellness) devices to household appliances. These hold great promise for enhancing people's lives, improving our health and well-being, and streamlining or automating a range of daily functions. They also, however, introduce a range of risks including external manipulation, data breaches, surveillance, and physical harm. While consumer devices are often subject to regulation, standards or codes, these have not previously incorporated the new challenges and risks that arise in IoT consumer devices.

The UK has been proactive in considering how current regulatory frameworks, best practices, guidance, and other resources can support the uptake of innovations in consumer IoT devices in a safe and secure way. Through the PETRAS Cybersecurity of the Internet of Things research hub – now the National Centre of Excellence for IoT Systems Security, we have worked to support DCMS to develop the Code of Practice for IoT Security (CoP). Seeing this work, alongside the significant contributions from multiple stakeholders, including industry, governments and civil society, contribute to the development of an ETSI Standard was exciting and a real demonstration of the value of interdisciplinary academic teams working closely with industry and policy makers to bring about positive change.

This work is not complete though. Adapting the standards, governance, and policy of emerging technologies is an iterative process that requires constant reflection, evaluation, analysis, and reconsideration as both the implementations develop and as our use (or misuse) of them evolves. This report picks out three issues that we feel require urgent consideration. The use of IoT devices by perpetrators of domestic abuse is a pressing and deeply concerning problem that is largely hidden from view. Collecting data (and therefore evidence) on this is challenging for a number of reasons outlined in this section by Leonie Tanczer. There are concrete steps that both industry and the policy community could take to address the misuse of consumer IoT in this setting and we include a number of these as well as lessons from other countries.

Fitness devices are also raising concerns as they have proven easy to compromise and they reveal deeply personal information about people's bodies, their homes and their movements. While IoT medical devices are regulated, there is a grey zone between these and fitness devices which results in a regulatory gap. Saheli Datta Burton has compared these two classes of devices, the ways they are vulnerable, the ways they are used, and the steps that could further secure fitness devices for the consumer market.

Finally, children's IoT connected toys are coming under new scrutiny as we realise the implications of embedded cameras and microphones for a child's (or parent's) protection and right to privacy. These connected toys have the potential for misuse and unauthorised contact with vulnerable minors. The British Toy and Hobby Association has responded to this by offering a range of guidance notes and by interpreting the CoP but with SMEs making up the bulk of IoCT manufacturing, there is plenty more to be done to ensure that these organisations are sufficiently informed and equipped to avoid producing and marketing insecure toys.

In Section 1 below, we address these three issues in turn and in Section 2 we provide some analysis of how widely the UK CoP has been taken up in various forms.

Section 1
Emerging Risks:
Consumer IoT
Security

At Risk: Victims and Survivors of Domestic Abuse

Introduction

An emerging problem connected to the widespread deployment of IoT technologies is their misuse in the context of intimate partner violence (IPV). In the last year, domestic abuse affected an estimated 5.7% of adults (2.4 million) in England and Wales (ONS, 2019). In the vast majority of cases, IPV is experienced by women and girls, which is particularly evident in intimate partner homicide cases, where women account for around 82% of victims and survivors (Smith, 2020; UNODC, 2018). This gendered dimension of violence is reflected in digitally-enabled forms of abuse (Woodlock, 2017). Digitally enabled IPV should not be considered as a "separate" abuse form, but instead, as part of a diverse set of patterns and structures used to control, coerce, and harm victims and survivors. Due to this intermediary role of technology, scholars and practitioners commonly define the phenomenon of abuse conducted through information and communication technologies as "technology-facilitated abuse" or "tech abuse".

While tech abuse is not an official concept or measurement category, tech abuse in IPV situations has been studied for some time (Markwick et al., 2019; Woodlock, 2014). Scholars have examined issues such as image-based sexual abuse cases (Citron & Franks, 2014; McGlynn, Rackley, & Houghton, 2017; McGlynn, Rackley, & Johnson, 2019; Walker & Sleath, 2017), the use of malicious software frequently referred to as "stalkerware", "spouseware", or "spyware" (Chatterjee et al., 2018; Freed et al., 2018; Harkin, Molnar, & Vowles, 2020; Khoo, Robertson, & Deibert, 2019), and gender-based harassment enabled through social media (Citron, 2009; Tanczer, 2013; Vitis & Gilmour, 2017). The focus of most research outputs is on conventional devices such as smartphones and laptops or services offered via the Internet. Research has also explored how new forms of victim-blaming are emerging (Harris & Woodlock, 2018; Mckinlay & Lavis, 2020). By advising affected parties to stop using devices or services, or by urging them to adjust their behaviour to circumvent such misconduct, the

responsibility is shifted from the perpetrator to the victim and survivor.

The need to protect IPV victims and survivors from the adverse effects of the use of IoT devices and services to facilitated abuse is of particular importance, as we are rapidly moving towards a far more interconnected environment (Tech UK, 2019). However, our understanding and awareness of tech abuse facilitated through IoT is still in its infancy. Internationally, only a handful of scholars and a selected number of support organisations have begun to explicitly address this topic (Slupska, 2019; Janes, Crawford, & OConnor, 2020; Mayhew & Jahankhani, 2020; Parkin et al., 2019; Leitão, 2019; Rodríguez-Rodríguez et al., 2020; Slupska & Tanczer, forthcoming).

IoT-Facilitated Tech Abuse

There is no agreed terminology to describe or to measure the abuse that is conducted through smart, Internet-connected systems. However, for the sake of simplicity, one can conceptualise this distinct form of tech abuse as "IoT-facilitated tech abuse". This abuse form sits within and overlaps with different categories - such as harassment or coercion and control - and is associated with a combination of behaviours (Dragiewicz et al., 2018), areas (Henry & Flynn, 2020), or dimensions (Powell & Henry, 2018) including monitoring, humiliation, and impersonation.

The risks that IoT technologies generate are not necessarily unique. However, IoT-facilitated tech abuse can expand and exacerbate abuse patterns as well as the reach of perpetrators far beyond the capabilities seen through smartphones or laptops (Figure 1). Specifically, the functionalities that IoT systems offer provide perpetrators with a range of avenues to monitor and control victims and survivors. IoT technologies can be disguised in terms of their ability to sense, process, and collect data. They can also learn patterns of behaviours and preferences, giving away sensitive details that can expose victims and survivors.

Furthermore, the capacity to control devices from afar showcases the physicality that is inherent to IoT. The ability to amend the material environment can become an avenue for "gaslighting" (Sweet, 2019). Perpetrators may adjust settings of devices from a distance; changing household lighting, heating, or door locks (Bowles, 2018)[A]. Perpetrators may also persuade victims and survivors that devices can or cannot perform certain activities such as the recording of video, audio or geo-location data. Both options can cause

---

[A]   The potential for this type of interference in a victim's and survivor's home connects directly with economic abuse. This can be exemplified in the context of consumer-based Demand-Side Response (DSR), which is an initiative promoted by the Department for Business, Energy & Industrial Strategy's (BEIS). A perpetrator's ability to increase a victim's and survivor's energy consumption during peak times could result in heightened energy bills.
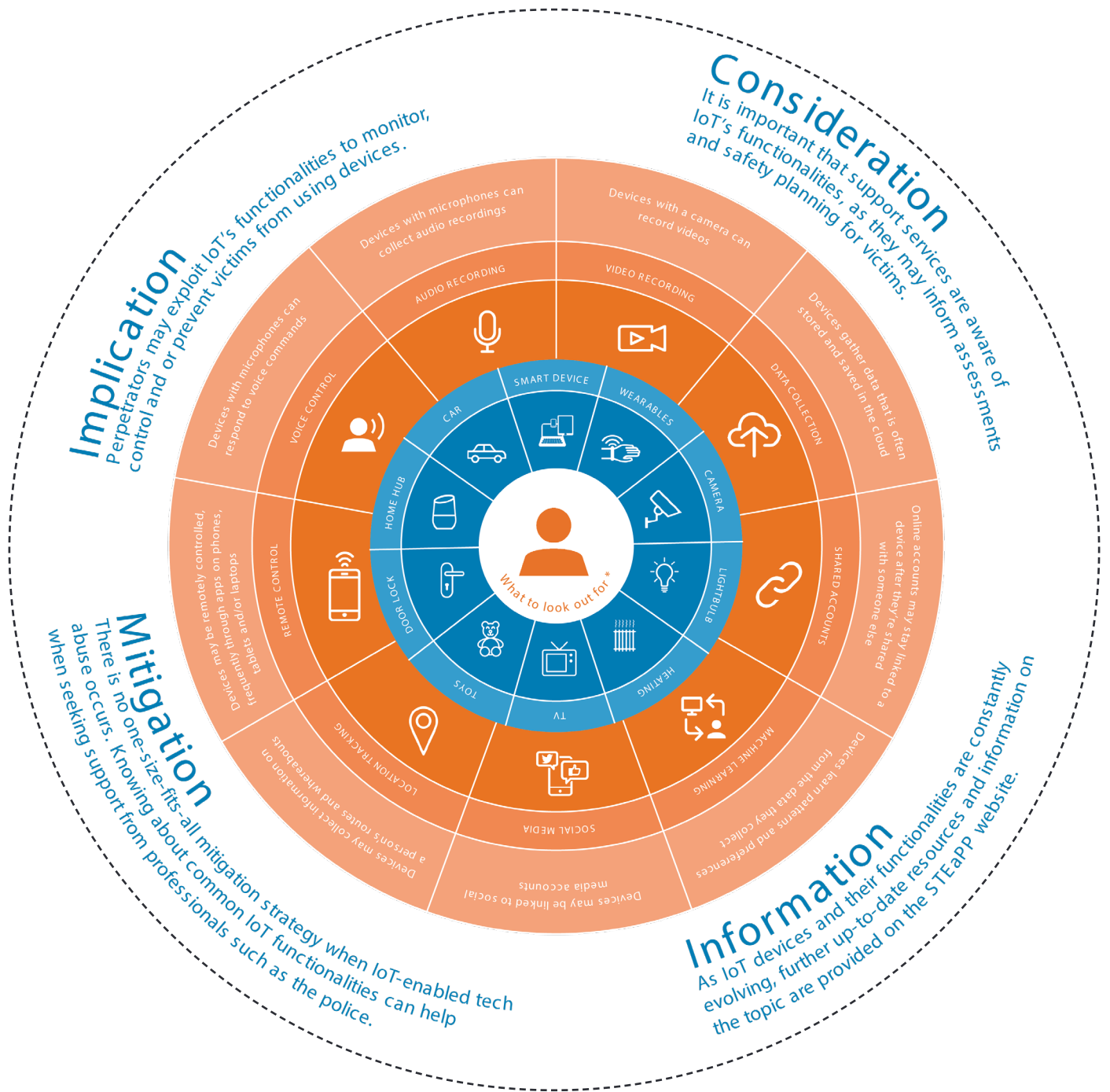
Figure 1: UCL's Gender and IoT (GIoT) Guide for the IPV support sector. This guide outlines some of the functionalities that can negatively affect IPV victims and survivors (Tanczer et al., 2018). Full version available online.

affected individuals to start questioning their own safety as well as the security level offered by their digital systems. Hence, an overestimation of IoT's surveillance capabilities as much as the underestimation of them can adversely impact vulnerable groups.

IoT devices are also built on the assumption of trust and implied consent - both between devices as well as between people. Therefore, the conventional threat models deployed by vendors do not sufficiently account for the risks created by IPV. These risks are not external but internal to the system. The insider status, together with the power and authority perpetrators uphold, equips abusers with unique access and privileges that most of the guidelines outlined in the current CoP will not address (Slupska, 2019). Hence, the ways in which IoT devices may be (mis)used for various forms of violence - including stalking, emotional, financial, physical, and sexual abuse - are not yet adequately captured.

Scale and Scope

Quantitative data on the scale and scope of IoT-facilitated tech abuse is currently non-existent. This is due to a range of challenges in the collection, identification, and analysis of tech abuse data more generally. **Firstly,** very few statutory or voluntary support services are explicitly documenting tech abuse through a tick-box or other dedicated question in their risk assessment and data management system (Tanczer et al., 2018). Instead, the relevant information is spread across several records that researchers are only now beginning to evaluate.

Secondly, IoT as a distinct technology is often not differentiated from other devices or digital platforms and is instead subsumed under the overarching umbrella term of tech abuse. There has been some limited quantitative research on tech abuse more broadly. For instance, the UK charity Refuge documented that 72% of its service users experienced abuse through technology in 2019 (Refuge, 2020). Similarly, a multi-sample study (2012–2018, n = 1137) conducted in urban areas of the southwestern United States found that 60–63% of victims and survivors reported having experienced tech abuse by an intimate partner (Messing et al., 2020). While such evaluations of tech abuse are beneficial (and more are needed), these all-encompassing results deflect from the nuances between different technical systems and make a longitudinal assessment of the rate and range of IoT as well as other technological abuse forms impossible.

Thirdly, the understanding of what IoT is and encompasses is not clear to everyone. This lack of comprehension manifests in a bias in the current evidence-pool. For instance, any data derived from notes, reports, and write-ups by humans (which includes data documented by frontline workers such as the support sector and police)

fail to capture the real extent of IoT-facilitated tech abuse. This dynamic has been observed by the "Gender and IoT" research team at UCL (Figure 2). As part of their online tech abuse survey with the UK IPV sector (which at the time of writing is still ongoing), they recognised that respondents often did not know whether IoT-facilitated tech abuse was taking place. Written responses aimed at contextualising participants' answers highlighted that respondents had conflated conventional digital technologies with IoT in their answers.

Due to these research difficulties, scholars have tended to rely on qualitative studies that have drawn on interviews and focus groups with victims and survivors as well as support organisations (Lopez-Neira et al., 2019; Parkin et al., 2019; Leitão, 2019). In these conversational settings, interviewers and facilitators can explain IoT to attendees and direct the conversation, which is not possible when analysing survey data nor secondary data from, for instance, police records. Nonetheless, in the long-term, quantitative studies on IoT-facilitated tech abuse will be needed. To achieve this, evidence-based definitions and measures that capture this form of abuse will have to be established. The latter will require clear thresholds on the exact context, patterns of behaviour, and consequences of tech abuse (Messing et al., 2020).

Frequency table

Choices	Absolute frequency	Cum. absolute frequency	Relative frequency	Cum. relative frequency	Adjusted relative frequency	Cum. adjusted relative frequency
Yes	33	33	29.73%	29.73%	62.26%	62.26%
No	9	42	8.11%	37.84%	16.98%	79.25%
Don't know	11	53	9.91%	47.75%	20.75%	100%
Sum:	53	-	47.75%	-	100%	-
Not answered:	58	-	52.25%	-	-	-

Average: 1.58	Minimum: 1		Variance: 0.67
Median: 1	Maximum: 3		Std. deviation: 0.82

Total answered: 53

Figure 2: Response Patters to IoT use. Question: "Have you already experienced IoT technologies (i.e., "smart", Internet-connected devices) being of concern when working with victims and survivors of domestic and sexual violence and abuse?"

Key Issues

Below are some pointers aimed at helping to develop much needed "IPV Threat Models" (Slupska & Tanczer, forthcoming), design principles, and guidelines which may support future iterations of the CoP to better incorporate a response to IoT-facilitated tech abuse:

Power imbalance
In abusive contexts, perpetrators tend to oversee the purchase, maintenance, administration, and disposal of devices (Leitão, 2019). As victims and survivors are frequently not the owner or account holder of products, they lack authority to make changes to the system, and often do not have the awareness and knowledge of how to amend settings[B]. While this should not portray victims and survivors as helpless, this power imbalance is foundational to all IPV situations and could potentially be even exacerbated by the Terms and Services typically deployed by IoT device and system suppliers. Yet, this asymmetry goes against common cybersecurity assumptions that rely on administrator rights, consent and authentication rules, and ownership (Slupska & Tanczer, forthcoming). Hence, while IoT systems functionality may benefit average users, smart capabilities can and are repurposed in IoT-facilitated tech abuse cases to the detriment of those that lack access, knowledge, and control. The implementation of settings that enable, for example multiple accountholders with clearly attributed and transparent rights and abilities, security and privacy push notifications, and demand users to regular re-consent to linking accounts and other features, could be beneficial.

User Interface (UI)-bound abuser
Research has shown that the typical tech abuser must be thought of as a "UI-bound adversary" (Freed et al., 2018), which means that rather than using sophisticated, technical methods, IPV perpetrators often repurpose ordinary functions and features to control victims and survivors. These include things like remote control, biometric authentication, or the option for shared user accounts. The deployment of these mechanisms for malicious intent means that these functionalities are not always given due consideration by "conventional" cybersecurity approaches as they are regarded as a feature rather than a vulnerability. A useful step would be to test technical systems before their deployment not only for their 'technical' security and privacy (through pen testing) but also for their possible 'societal' impact in terms of their usability possible unintended negative consequences.

B   A similar power dynamic often applies when third parties with "legitimate" access to premises (such as landlords) are involved, although a discussion of this is beyond the remit of the IPV context discussed here.

Centralisation

The increasing drive to expand the connectivity of devices and provide centralised hubs such as smart speakers creates nodes that are "information goldmines" for perpetrators. In addition, research has shown that IoT manufacturers do not provide transparency and the necessary prompts to flag up to IoT device users the breadth of connections and access controls they have agreed to (Janes et al., 2020; Parkin et al., 2019). People may not remember with whom they have shared credentials, and they may have no easy way of checking this which can provide avenues for abusers to continue to spy on their family or ex-partner covertly and over an extended period of time. IoT devices should have simple ways for users to ascertain who has access and through which channels.

Usability

Previous studies have indicated a range of interventions that device manufacturers can implement to improve the usability of IoT devices in ways that will benefit victims and survivors. These include suggestions mentioned above, plus more accessible and navigable user interfaces, improvements to the usability of privacy and security controls, enforced authentication requirements, and the ability to review historical queries and actions (Janes et al., 2020; Parkin et al., 2019; Leitão, 2019).

Three phases of IPV

The implementation of better safety and security features to tackle tech abuse must account for the three phases of IPV (Matthews et al., 2017). While this model is not applicable to all forms of abuse and offers a simplified portrayal of complex dynamics[c], it does provide an anchor point to think about the diverse privacy and security expectations devices and systems must tackle. The needs and risk that individuals face before, as well as during a "physical control" phase (Phase 1) are different from those during the "escape" (Phase 2) and again, the following "life apart" phase (Phase 3; see Figure 3). According to our research, perpetrators commonly misuse IoT systems in the earlier abuse stages against victims and survivors (e.g., because they are the owner of devices and/or exert control over victims and their digital systems). However, the exact same functionalities (e.g., geo-location tracking, video recording) that perpetrators may misuse against victims and survivors during the "physical control" phase may benefit victims and survivors whenever they have separated themselves from violent partners and begin to feel in control of their lives as much as the technical features these systems now can offer them.

Perpertrator focused solutions

There is little work on how IoT technologies are being used by perpetrators or on how they may be better designed

---

C   The model assumes a spousal relationship. We acknowledge that it does not translate to forms of, for example, parental abuse where additional layers of complexity come into play.

to challenge them (Bellini et al., 2020; Bellini et al., 2019; Tanczer et al., 2018; Tseng & et al., 2020). Instead, most technical solutions are aimed at assisting victims and survivors in changing their behaviours and amending settings to escape risk scenarios. Future efforts must tackle the discrepancy in focus and instead pro-actively challenge and prevent perpetrators from abusing tech rather than re-actively intervene by asking victims and survivors to adjust.
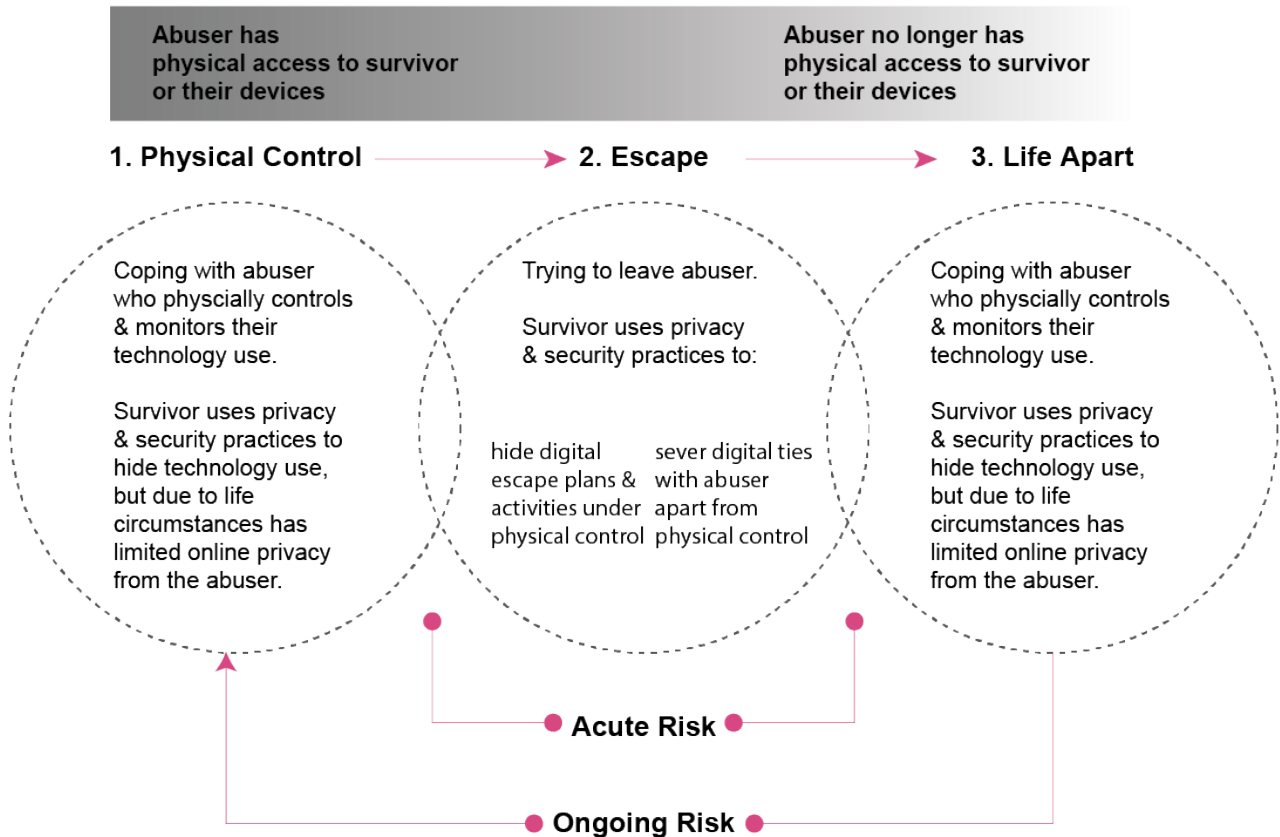
Figure 3: Three phases of IPV that affect technology use.
(adapted from Matthews et al. 2017b)

Policy Directions

Based on the current level of knowledge, a range of possible actions may be taken that can help improve the response of policy makers, industry, and the IPV support sector. With regards to policy measures, different documents, legislative developments, and strategies must be aligned.

Firstly, an updated CoP needs to align with the Online Harms White Paper. However, the White Paper is currently limited to harms derived from online platforms and, thus,

falls short on the role of IoT systems and devices (Tanczer et al., 2018). Both documents will have to shift focus, with the CoP requiring a stronger emphasis on IPV-focused, and the Online Harm White Paper on IoT-facilitated risks.

Secondly, the CoP must foster the ambitions set out in the Domestic Abuse Bill. The latest version of the Bill is meant to have been future-proofed (Tanczer, 2019) and should now account for abuses conducted via smart devices and gadgets. Additionally, the soon-to-be-published Violence Against Women and Girls as well as the Domestic Abuse Strategy can direct the guidance of the CoP. All these activities should, of course, align with global developments such as the EU Cybersecurity Act, which establishes an EU-wide cybersecurity certification framework for digital products, services and processes.
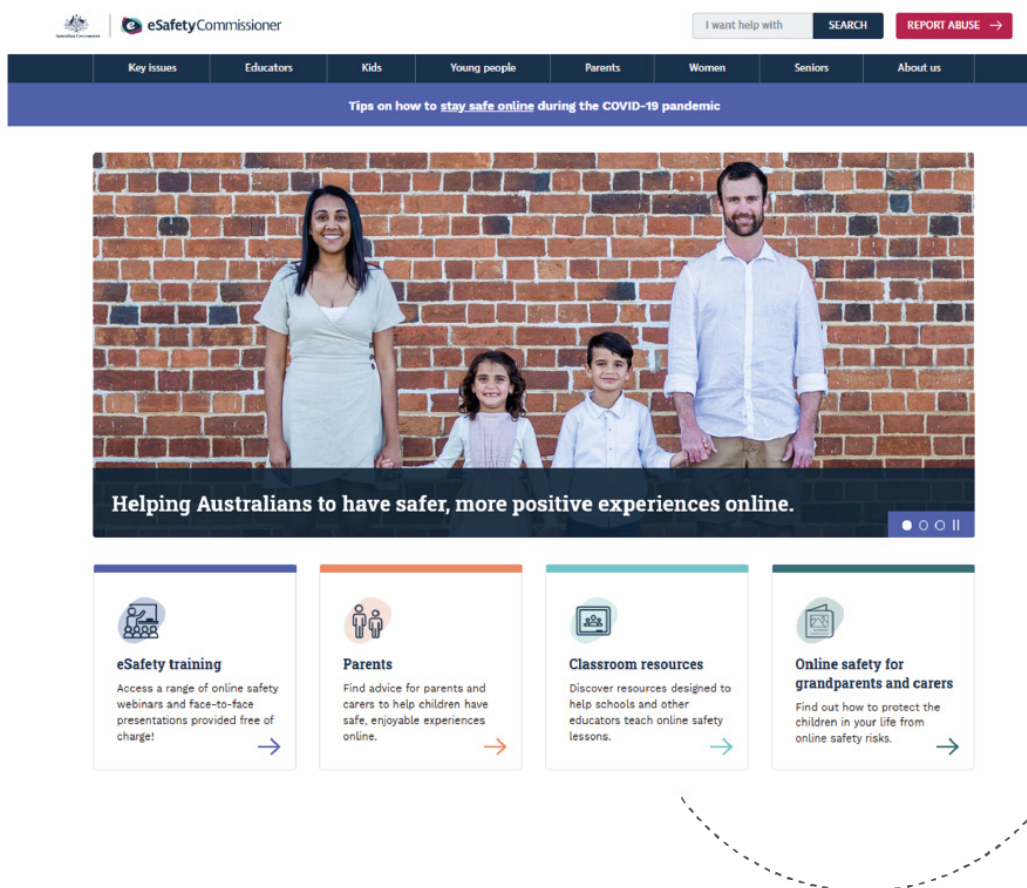
Figure 4: The Office of the eSafety Commissioner, Australia: support for the public
The Office of the eSafety Commissioner is Australia's central body that can be used by the public to receive information on online safety, make complaints, and find help and support. It also has the legislative power to enforce better safety and security practices.

The UK Government may also take note of recent actions by the Australian Office of the eSafety Commissioner. This is a centralised public body that provides information, help and support for the Australian public about online risks and harms. For instance, the eSafety Office promotes online safety education for a variety of communities (e.g., teachers, kids, parents, women, seniors), can remove inappropriate content found online, liaises with tech vendors to help mitigate risks, conducts research and develops public-facing resources, and generally acts as a one-stop shop for any member of the public.

A body with similar roles and responsibilities is missing in the UK where citizens lack a streamlined contact point for issues such as online bullying, online hate crime or best practices around cybersecurity. Whilst some of these functions may be taken on by UK's National Cyber Security Centre, the NCSC, the Information Commissioner's Office, the ICO, or the police – to date - neither of these bodies offer the same mediating and public communication functions that the Australian Office of the eSafety Commissioner upholds. To achieve a similar alignment, UK Government policy teams working across different department and agencies could assist in facilitating such coordination efforts.

While the voluntary sector tends to favour initiatives from the specialist support sector, there are benefits to centralised government initiatives and a more streamlined approach to tech abuse. Throughout the research conducted at UCL (Tanczer et al., 2018), frontline organisations have expressed an interest in seeing more specialist tech abuse assistance. This may be facilitated through the establishment of dedicated tech abuse units in police forces and support services, and/or through a hotline that could sit, for example, within the NCSC. The latter has already worked in collaboration with the GIoT team and developed a short IoT guide that is available to IPV support organisations.

Some industry actors are now beginning to tackle the issue, although their activities are not specific to IoT-facilitated abuse. For example, IBM recently released five "coercive control resistant" design principles, which are intended to prevent developments from being used for domestic abuse (Nuttall et al., 2020). Google's Security & Privacy Research & Design Group has produced various outputs on the issue of tech abuse (Matthews et al., 2017a, 2017b; Sambasivan & et al., 2019a, 2019b, 2019c) and, prompted by research findings, taken action against some spyware apps that were available on its app store (Chatterjee et al., 2018). Kaspersky, F-Secure and other anti-virus and cybersecurity providers have recently established a dedicated "Coalition against Stalkerware". This includes various IPV frontline organisations that have the expertise and experience to advise and guide the development of interventions.

Figure 5: Digital security training event for the IPV support sector held in London in 2018 (UCL STEaPP, 2018).

More industry-wide activities that are driven by the sector and fostered by umbrella organisations such as the IoT Security Foundation, the Alliance for the Internet of Things Innovation (AIOTI) or the Global System for Mobile Communications Association (GSMA) may be helpful for addressing IoT-facilitated tech abuse. This could ensure that activities are aligned, as well as relevant data and response mechanisms shared across vendors. Companies may also take an example from the Australian Communication Alliance, which developed industry guideline to assist customers who experience domestic and family violence (Communications Alliance Ltd, 2019). As IoT manufacturers will have to respond to IPV victims' and survivors' requests to withdraw or restore access or change system settings, the sector must know how to effectively and appropriately engage with such vulnerable communities.

Lastly, the voluntary and statutory support sector is urged to change its risk assessments and safety practices (Tanczer et al., 2018) to both assist in the better collection of data and also to react to the changing risk landscape as smart systems become more prevalent. The above-mentioned helpline or the establishment of "Tech Abuse Clinics" as trialed in New York (Havron et al., 2019), implemented by the City of Vienna (Stadt-Wien, 2020) and tested under the banner of a "CryptoParty" in London (UCL STEaPP, 2018) may offer useful avenues. Such a centralised tech service – which must cater both urban and rural areas - could further be bolstered through its combination with other support provisions that existing support sector organisations offer, including legal, mental health, or housing advice. However, funding to support capacity building and the development of specialist support services is much needed and will be essential to an effective response to the looming rise of IoT-facilitated tech abuse (Womens Aid, 2020).

At Risk: Users of Fitness Devices

Introduction

One of the more heavily researched areas of the IoT includes medical devices and the potential for significant benefits of connected, interconnected, and remote medical care. Connected medical devices are increasingly ubiquitous, ranging from large stationary equipment like imaging machines in hospitals and clinical settings, to small wearable devices like heart rate monitors, and those actually implanted inside the human body like pacemakers. These are often collectively referred as the *Internet of Medical Things* (IoMTs). Like most aspects of the medical sector, IoMTs are regulated in some jurisdictions, e.g. the UK, US, and EU (ISO., 2006; MDCG., n.d.; MHRA, 2014; USFDA, n.d., 2019b, 2019c).

Also growing in popularity and use are less regulated connected fitness devices aimed at the consumer market. These devices promise many benefits for users; from monitoring vital health data like insulin levels, oxygen saturation etc. to tracking fitness metrics for healthier lifestyles like counting footsteps taken, calories burned. By 2017, *Fitbit* - the popular fitness wearable alone had 25 million users (Fitbit, 2018). However, fitness devices do not fall under the regulatory frameworks applied to medical devices. In some cases, the line between medical devices, which are regulated, and fitness devices, which are not, is less than clear. Indeed, the manufacturers of fitness devices must declare if the device is medical or fitness for regulatory purposes (discussed later).

Somewhat problematically though, very little differentiates the communication architecture of IoMTs from the less regulated connected fitness devices (Figure 6). Both have embedded sensors that read user health data and relay it remotely to health delivery organisations (HDOs) like hospitals and clinics in the case of medical devices. This relaying of data typically happens via mobile applications ('apps') using existing short-range communication technologies over wireless (e.g., wi-fi, bluetooth, zigbee, or other radio technologies in the ISM (industrial, scientific and medical) band or cellular (e.g., GSM) connectivity (Alsuwaidi et al, 2020; Atzori, Iera, & Morabito, 2010; Malan et

al, 2004; Memon et al, 2020). In the case of data generated by medical devices, HDOs in turn, monitor vital signs and relay healthcare information (e.g., insulin dosage), increasingly in real time, back to user-held medical devices which then affect some change (e.g., dispense medicine). Through these actions, vast amounts of health data can end up stored in virtual 'clouds' (Atzori et al., 2010; Doukas & Maglogiannis, 2012). For the purposes of this report, the key point is that both fitness and medical devices (whether user-held or standalone equipment in health institutions) share the interconnected cyber 'commons' where cyber-threats and cybercriminals make little distinction between regulatory categories. Instead, ever-expanding interconnectedness and interoperability between discrete device categories amplify regulatory (and oversight) gaps that expose publics to layers of security vulnerabilities at device, network, and storage levels.

For the purposes of this report's focus on 'consumer IoT device cybersecurity', we focus on connected fitness devices available for consumers via retail outlets including online marketplaces (UK-CoP, 2018). A discussion of user-held 'medical devices' typically intended for patients with a clinically assessed need for it and available through (non-consumer) institutional channels in health(care) such as hospitals and clinics is beyond this report's remit (see e.g., NHSDigital, 2020). Nevertheless, given the shared cybercommons between device categories, overlaps in the evolving cybersecurity landscape facing each are inevitable. Thus, a discussion, that, in some dimensions, includes both fitness and user-held medical devices, is oftentimes considered useful and appropriate in understanding the evolving security and safety challenge confronting users. In the next section, we briefly present the security vulnerabilities at device, network and storage levels faced by both device categories followed by a discussion of the key vulnerability drivers. Finally we conclude by reflecting on standardisation of secure manufacturing for addressing security and safety concerns.

Device level vulnerability: easy to hack
Design flaws in the manufacturing of connected fitness and user-held medical devices that make them easier to hack increase their vulnerability to cyberattacks. Several security researchers such as Kevin Fu, Jay Radcliffe, Billy Rios and Jonathan Butts have demonstrated the risks in public forums by hacking into a connected implantable heart defibrillator (University-of-Massachusetts-Amherst., 2008), insulin pump (Mills, 2011; Radcliff, 2019) and an implantable pacemaker (CBSNews, 2018) respectively. These demonstrations raised critical public awareness of the security design flaws in medical devices including alerting the FDA to these issues, specifically the lack of basic encryption and user authentication. In particular, 'hacking' demonstrations by various security researchers highlighted the ease of hacking into these devices

Cloud storage

Health delivery organisations

Fitness Devices

Medical Devices

Figure 6: The Shared CyberCommons

(Davis, 2018b). For instance, as highlighted by Rios' and Butts' cautionary note that they are "yet to find a [user-held medical] device that [they]'ve looked at that [they] haven't been able to hack" (CBSNews, 2018). Yet, despite this long history of demonstrating vulnerabilities in these devices, as recently as June 2020, the US Department of Homeland Security issued a security alert highlighting the lack of encryption and its safety implications for Medtronic pacemakers and defibrillators - both 'medical devices' (US-DHS, 2020). In this case, the Conexus telemetry protocol utilised within this ecosystem did not implement encryption. As a consequence, "an attacker with adjacent short-range access to a target product [could have] listened to communications, including the transmission of sensitive data" (ibid).

Fitness devices that may appear to have less critical implications for healthcare share the same vulnerabilities as they continue to be developed and marketed with little effort to address even basic design vulnerabilities that make them easy to hack. For instance, popular devices such as **Fitbit** (Cyr et al, 2014; Rahman, Carbunar, & Banik, 2013), **smartwatches** (Norwegian-Consumer-Council, 2017; Rawlinson, 2015) and various other wearable devices (Tolentino, n.d.) have been found to contain design vulnerabilities related to insecure authentication etc. (see e.g., Ching & Singh, 2016). In the wrong hands, such vulnerabilities could compromise user security and safety. For instance, fitness or wellness devices, namely **Digitsole Warm Insoles, Modius Headband and Ivy Health Kids Thermometer**, have revealed that aside from all "collecting and exposing personal information", physical harm could be caused by hackers by altering the temperature and electric pulse (leading to nausea and sickness in the Digitsole and Modius devices respectively) (VPN Mentor, 2020).

Key network and storage level vulnerability: increased attack surface
In addition to device level vulnerabilities, interconnectedness between devices sharing networks and clouds exacerbate design vulnerabilities by expanding the attack surface, at times exponentially. In March 2020, researchers detected 12 vulnerabilities (named "SweynTooth") in the Bluetooth Low Energy (BLE) communication technology used by nearly 480 medical devices across the world that could have allowed hackers to "crash, deadlock [or freeze and] bypass security function available only to authorised users" (USFDA, 2020).

Figure 7: "Sweyntooth" vulnerability in March 2020 *Source*: Cybersecurity & Infrastructure Agency

While no known instance of patient harm was reported from Sweyntooth, the FDA's acknowledgement of the 'significant' "risk of patient harm, if such a vulnerability were left unaddressed highlights the unprecedented patient safety risks that accompany the global expansion of interconnected devices (Doffman, 2019). Kingsley Manning, former chairman of NHS Digital, perhaps summarised it best when he cautioned that:

> The problem with cyber security for the NHS is [that] it has a particular vulnerability… It's very interconnected so if you get an attack in one place it tends to spread" (BBC, 2017).

Critical security design flaws and the challenges of interconnectedness are not unique to connected fitness or medical devices but a concern for IoT devices more generally. However, the pressures and imperatives that drive these key vulnerabilities differ across sectors and an understanding of the sector-specific drivers (perceptions, attitudes, barriers, and gaps) impacting fitness and user-held medical devices are key considerations for future policy and briefly discussed below.

What is driving vulnerability?

Low risk perception

The absence of any known events of physical harm to users of fitness and user-held medical devices from cyber attacks - such as remote alteration of dosage etc. - has fostered a low (cyber)security risk perception of user-held devices whether for fitness or medical purposes (Clearswift, 2019; Gottlieb, 2018; Hockey, 2020; Medtronic, 2020). The assumption that attackers are likely to target large deep-pocketed organisations that offer better payoffs than individual patients (Cyberdefense., 2019; Hockey, 2020; Schwartz, 2016; Verizon, 2020) has further bolstered this view based on the logic of financial gain as the overwhelming motive behind cyber attacks (in 86% of breaches across 27 countries in Verizon, 2020). In turn, low (cyber)security risk-perception plays a significant role in industry, investment, and regulatory attitudes across the UK, US, and Europe (discussed next).

Investment attitudes

Underinvestment trends in the cybersecurity of the healthcare sector more generally, is reflected in the fitness and medical devices space (Davis, 2018a; IoT Business, 2019, 2020). Most of this investment tends to prioritise the cybersecurity of medical devices in hospitals and clinical settings. A focus on 'large scale, multi-patient' centres is explicitly encouraged by regulators as reflected in Dr Scott Gottlieb, FDA commissioner's statement in 2018:

> The FDA isn't aware of any reports of an unauthorised user exploiting a cybersecurity vulnerability in a medical device that is in use by a patient. But the risk of such an attack persists. ...The goal is to give product developers more opportunity to address the potential for large scale, multi-patient impact that may raise patient safety concerns (Gottlieb, 2018).

For health development organisations (HDOs), these investments have been in large part spurred by the need to protect hospital infrastructure against the wide-ranging fallouts experienced after a rash of highly publicised **(ransomware) attacks** (Irdeto, 2019; Moganedi, 2018; Novinson, 2020; Swinhoe, 2020; Zahra & Chishti, 2019) including from **privacy breaches**, **reputational and other damages**, and the **rising costs of litigating compensation** for these (Davis, 2019; Scammell., 2019). Meanwhile, attention to and investment in the security of fitness and user-held medical devices have suffered, reinforced by widely held low (cyber)security risk perception of these devices (Clearswift, 2019; Gottlieb, 2018; Hockey, 2020; Medtronic, 2020).

Economic and operational barriers

Secure manufacturing involving some form of basic inbuilt encryption, password protection before distribution, user authentication (e.g., multi-factor authentication) to regular audits and assessments is widely viewed as industry best practice for securing IoT devices including fitness and medical devices (Arora, Yttri, & Nilsen, 2014; CBSNews, 2018; Clark & Jeremy, 1996; Jonsson & Tornkvist, 2017; Lord, 2020; Yaacoub et al., 2020). However, the routinisation of secure protocols in manufacturing practices for secure fitness and user-held medical devices remains constrained by implementation challenges hinged on manufacturer's economic and operational considerations.

In particular, industry-wide practices of 'patch management' (using software patches to update devices) for securing user-owned devices over device lifetimes (typically 2 to 4 years) (IHE., 2015) is an economically attractive option for manufacturers. This is because patch management it is relatively easier to implement and requires relatively low upfront investment (often delivered via tie-ups with third party 'patching' providers) (Samani, Honan, & Reavis, 2015; Seagren, 2011; Shinder, Diogenes, & Shinder, 2013; Williams, 2014; Winkler, 2011). This is especially relevant in comparison to the substantial skills- (e.g., in secure coding), capital- and time- resources needed to operationalise secure manufacturing which push up retail prices of fitness and medical devices. This in turn raises competitiveness concerns among manufacturers, especially among those aiming for faster (Ponemon-Institute, 2017, p. 2) and cheaper market entry for their products (Oberhaus, 2020).

Despite the comparatively lower costs, 'patching' is widely considered an imperfect security solution; it is essentially reactive, based on a "don't fix it if it isn't broken" approach and highly uneven in its application based on manufacturer's capacity and their subjective commitment to security or assessment of its immediacy (Seagren, 2011) (see also Samani et al., 2015; Shinder et al., 2013; Williams, 2014). According to Ponemon Institute's 2017 survey, only 9% (of 5996) medical devices manufacturers surveyed even conducted the annual cyber security tests necessary to understand where vulnerabilities lay (a critical tool for assessing where patches are needed)(Ponemon-Institute, 2017)[A]. In this sense, secure manufacturing provides a proactive approach that reduces the unevenness associated with patching by building security features into devices.

A further challenge is that few manufacturers and service providers have so far invested in "significant steps

---

A   Furthermore, "Testing of medical devices rarely occurs" says (Ponemon Institute, 2017, pp. 2). "Instead, 53% of HDOs do not test (45 percent) or are unsure if testing occurs (8 percent) and 43% of manufacturers do not test (36 percent) or are unsure if testing takes place (7 percent)" (ibid).
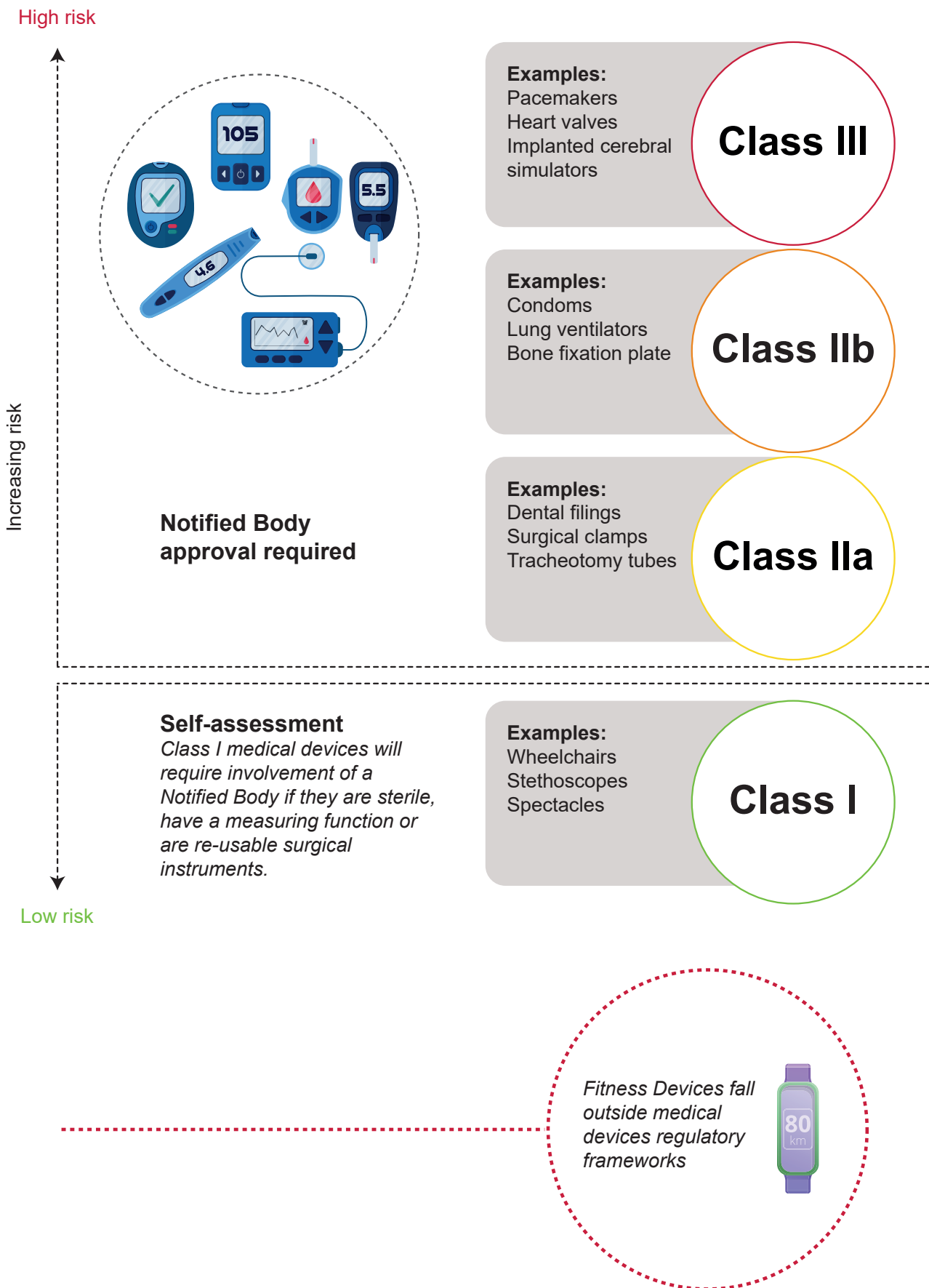
to prevent attacks" (Ponemon-Institute, 2017) such as secure manufacturing, whether due to low security risk perception, economic-operational barriers etc. However, this attitude may be changing towards incorporating the costs of better security features in business models (Irdeto, 2019). One indicator that highlights the 'inevitability' of a cyberattack (or its costs) in the minds of supply-side actors in the connected medical device space - is the increasing number of financial insurance products now being marketed to insure supply side actors against costs of cyber attacks (Maddox, 2015) or under consideration by insurers (Lloyds, 2018). Yet, whether this short-term and comparatively cheaper measure of insuring against financial fallout of attacks will eventually lead to a shift among manufacturers towards long term investments in preventive measures against attacks (e.g., secure manufacturing practices) is yet to be seen. The recent EU Cybersecurity Act establishing the EU Cybersecurity Certification Framework for manufacturers and developers of ICT products for the EU market is expected to incentivise investments in the security of consumer IoT (Bernabeu, 2019; EUaC, 2020).

Regulatory gaps
A frequent assumption is that fitness devices are more secure than other IoT devices by virtue of being regulated under the extensive standards and regulations covering medical devices (Best, 2018; Rosenblum, 2015). In reality, fitness devices are largely industry self-regulated across US, UK, and EU markets (i.e., they typically fall outside the purview of medical devices regulations) with few meeting even basic cybersecurity standards.

In the UK, the *Medicines and Healthcare Products Regulatory Agency* (MHRA) regulates medical devices based on risk to patients and users (from highest risk Class III devices to low risk Class I devices). Devices that meet the definition of a 'medical device' must demonstrate conformity with relevant essential requirements, although routes to conformity differ based on risk classification. Class I medical devices are self-certified against the requirements of the *Medical Devices Regulations* unlike assessment of higher risk devices which require the involvement of a *Notified Body* (MHRA, 2014). While the hardware element of fitness devices such as smart-watches, fitness trackers etc. that typically go by non-medical descriptors such as *wellness, wellbeing or fitness* devices do not qualify as a medical device (discussed earlier). In other words, manufacturers **self-assess** the risk-benefit of their products to **self-claim** its purpose as a (non-medical) fitness device. Thus, a smart-watch is a fitness device (but not a medical device) if its manufacturer claims all it does is read heart-rate without any medical (diagnostic or therapeutic) purpose. Nevertheless, manufacturers must apply *Conformité Européene* (CE) marking for all relevant regulations they meet such as for telecommunications

High risk

Increasing risk

Low risk

Examples:
Pacemakers
Heart valves
Implanted cerebral
simulators

Class III

Examples:
Condoms
Lung ventilators
Bone fixation plate

Class IIb

Examples:
Dental filings
Surgical clamps
Tracheotomy tubes

Class IIa

**Notified Body
approval required**

Self-assessment
*Class I medical devices will
require involvement of a
Notified Body if they are sterile,
have a measuring function or
are re-usable surgical
instruments.*

Examples:
Wheelchairs
Stethoscopes
Spectacles

Class I

*Fitness Devices fall
outside medical
devices regulatory
frameworks*

Figure 8: Medical Devices Classification by risk to patients. Adapted from MHRA,
Classification: An introductory guide to the medical device regulation (MDR), 2017

23

equipment[B]; this provides some assurance of quality for users even though compliance requirements for the CE regime or general product safety regulations (e.g., the UK's *General Product Safety Regulations 2005*) are less than that required for 'medical devices'. Within this governance framework, there has been a trend to increasingly tighten the security of software or mobile apps with therapeutic or diagnostic medical purpose (ISO., 2006; MHRA, 2014, p. 6; USFDA, n.d., 2019a). The US Food & Drug Administration (FDA) (USFDA, n.d., 2019c, 2019b) and the European Commission Medical Device Coordination Group (MDCG., n.d.) take broadly similar self-regulatory approaches with some jurisdiction-specific nuances for wellness devices.

A key advantage of choosing the fitness route is that it cuts down compliance cost burden for manufacturers. This undoubtedly makes retail prices more competitive but also appears to have so far adversely opened the market to low-security devices such as **Google-Glass** (now withdrawn) (Safavi & Shukur, 2014), **Fitbit** (Cyr et al., 2014; Rahman et al., 2013), **Samsung smartwatch** (Rawlinson, 2015) which continue to be developed and marketed with little effort to address basic design vulnerabilities. In the case of user-held 'medical devices', if and when (cyber) security vulnerabilities are found manufacturers provide regulators with public safety notices that the regulator then publishes on its website (to alert the public)[C]. However, regulators do not receive such notification for security vulnerabilities for 'non-medical' fitness devices and it is left to the manufacturer to notify users in such instances. A stronger measure of product 'recalls' has at times been used by the USFDA[D] for user-held medical devices that failed to meet security standards e.g., implantable insulin pumps, cardiac pacemakers etc. (USFDA, 2019a). However, neither safety alerts nor recalls or corrective actions (in the EU) have so far lead to industry-wide improvements in connected fitness or user-held medical device cybersecurity practices.

The point here is not that health and medicines regulators should extend their jurisdiction to consumer products such as 'wellness' devices. Overextending health regulatory expertise to non-medical jurisdictions raises questions

---

B   The General Data Protection Regulations (GDPR) may also apply in some instances.
C   In the UK, the MHRA publishes Field Safety Notices (FSNs) on its website and follows up FSN reconciliation process directly with manufacturers to address safety risks to users. MHRA can also issue independent advice to the public in relation to FSNs and depending on how effectively manufacturers carry out the Field Safety Corrective Actions (see footnote G) related to these.
D   In the EU, Field Safety Corrective Action (FSCA) is taken by a manufacturer to reduce a risk of death or serious deterioration in the state of health associated with the use of a medical device that is already placed on the market. Such actions, whether associated with direct or indirect harm, is reported by manufacturers to the MHRA and notified via FSNs (see footnote F). Guidance for manufacturers developed at European level (MEDDEV 2.12-1 rev 8) provides guidelines on medical device vigilance systems.

Medtronic

Medtronic Limited
Building 9
Croxley Park
Hatters Lane
Watford, Herts
WD18 8WW
www.medtronic.co.uk
Tel: 01923 212213
Fax: 01923 241004

Urgent Field Safety Notice
SmartSync Device Managers supporting
Azure™ pacemakers, and Percepta™, Serena™, Solara™ CRT-pacemakers
Software Update

June 2020

Medtronic Reference: FA917

Dear Healthcare Professional / Risk Manager,

Medtronic is writing to inform you of software updates available for SmartSync Device Managers supporting Medtronic Azure™ pacemakers, and Percepta™, Serena™, Solara™ cardiac resynchronization therapy pacemakers (CRT-P).

This update addresses a rare communication sequence during the first device interrogation with a SmartSync Device Manager that may result in the temporary suspension of some device features (i.e., battery measurements, Capture Management™, Atrial Lead Position Check™, EffectivCRT™ algorithms, and AdaptivCRT™). This rare interaction results in temporary suspension of automatic threshold testing and output adjustments, and suspension of auto-optimization of

Figure 9: Medtronic issued Field Safety Notice published on MHRA website
Source: Medicines & Healthcare products Regulatory Agency

of whether it would constitute an efficient allocation of scarce public resources intended for specialist purposes. Rather, the point here is that some form of innovative intervention (such as the CoPs basic security standards) is needed to address the gaps in oversight of the hardware components of 'wellness' devices[E]. Such interventions would contribute towards the security and safety of the rapidly expanding numbers of 'wellness' device users as well as go some way towards mitigating the risks of attacks to the wider healthcare infrastructure via these devices.

E   IoMTs and mobile applications with 'medical purpose' already fall within the regulatory purview of UK MHRA, US FDA and EC MDCG.

Where the UK CoP can help

Where fitness devices are concerned, the UK CoP comes at an opportune moment to support manufacturers in developing meaningful resilience, (beyond buying data breach insurance) from cyber-related business threats as well as protecting patients. A legislated and enforced UK CoP would not only remove secure-by-design features as a competitiveness concern (by mandating its compulsory inclusion across all IoMT manufacturing) but thereby also play a role in raising industry standards globally as baseline security requirement in emerging cyber-secure business models (Brass et al, 2018).

Where securing networks and clouds are concerned, the CoP similarly extends a recent turn from unfettered interoperability towards risk-based segmentation of interconnectedness through firewalls and access restrictions within a 'zero trust architecture' (ZTA). In ZTA, "devices only interact with other devices or systems with which they explicitly need to communicate" (Christopher Frenz, Infrastructure Director, Interfaith Medical Center in Tynan, 2017). Erik Devine, Chief Information Security Officer of Riverside Health, Chicago, notes that,

> Every application, every .dll file, every .exe, every patch [is manually restricted] ...If a doctor plugs in an iPhone and downloads iTunes, we're like, 'Nope, you can't do that.' Users can make requests and ask permission, but it's a manual process. ...We segment them down to the port ...We can say this machine only talks to this IP address on that port, and that's it (Tynan, 2017).

Guidance for safely migrating existing e-infrastructures to ZTA[F] just released by the US National Institute of Standards and Technology in August 2020, highlight the seriousness of the turn towards (micro)segmentation (Scott et al., 2020). Even 'physical' segmentation by physically limiting IoMT signals of a wearable device to its wearer's body are being tested (Das et al., 2019). In this scenario, the CoP offers a regulatory mechanism of segmenting the attacker from its target via secure manufacturing.

F   Zero trust networks (which are related to ZTA but not an identical concept) use encrypted network links and each endpoint authenticates to those they communicate with. If the authentication is incorrect, the network packets do not enter the receiving device. The worry is that with many devices, particularly battery devices, a zero trust network may not be appropriate given the amount of encryption, decryption, storage etc. that a resource constrained IoT device would be required to use.

Where the governance of fitness devices are concerned, the UK CoP would extend regulatory attention towards greater industry accountability via public registries of fitness devices envisaged by the UK MHRA[G]. Studies reveal that registration of consumer products with public registries run by public institutions (perceived as independent and impartial) serve as important 'accreditation' and 'validation' tool for manufacturers to gain consumer confidence (Dehmer et al., 2016). Likewise, a public registry of UK CoP compliant IoTs devices would foster public awareness of compliant and unregistered (hence non-compliant) products out there (see e.g., discussion of public's responsibility towards own security in (Blythe & Lefevre, 2016; Jackson Jr & Rahman, 2019).

Conclusion

In sum, standardising the security compliance criteria for consumer IoT (as the UK CoP aims to do) would essentially be a first step towards:

(a) extending regulatory coverage to the hardware element of fitness devices so far outside the remit of current medical devices regulation (see e.g Downey, 2020; RAENG, 2018),

(b) focusing supply-side attention on the cybersecurity (and safety[H])of users so far neglected in efforts focused on "large scale, multi-patient impact" (Gottlieb, 2018), and

(c) managing the end-point security risk to the wider health infrastructure via low security fitness and user-held medical devices (end-points).

G   Registries of devices with a stated 'medical purpose' already exist but tracking down a device registry is difficult as EU-based manufacturers can register in any EU member state.
H   Patient safety in medical devices regulation is a broad concept encompassing physical harm but also extends to adverse impact of cyber attacks e.g. on mental health (Clark et al., 2017; personal communication with MHRA specialist in August 2020).

At Risk: Children

Introduction

Internet of Children's Things (IoCT) includes a wide range of everyday artefacts with internet connectivity that are intended for use by children or in caring for them such as toys, learning development devices, and baby or child monitors[A]. While these devices offer a range of advantages through their connectivity, they also expose children and their families to safety and security risks that have not yet been fully articulated (see e.g., previous section on the challenges of interconnectivity in health and medicine). Mattel's *Hello Barbie*, launched in 2015 in collaboration with startup Toytalk, was perhaps the world's first IoCT toy that could not only converse with children using internet connectivity and speech recognition but could also 'listen' to them. *Hello Barbie* also allowed parents to login later and listen to their children's conversation with the toy. Children have always shared their secrets with their favourite toy (Adhikari, 2015) which, for some, raises ethical questions around whether "parents had the right to listen in" (Russell, Pettit, & Mize, 1998). However, when the toy is connected, a more worrying concern is who else could listen in, record, and store conversations, behavioural, and location data, and for what purpose?
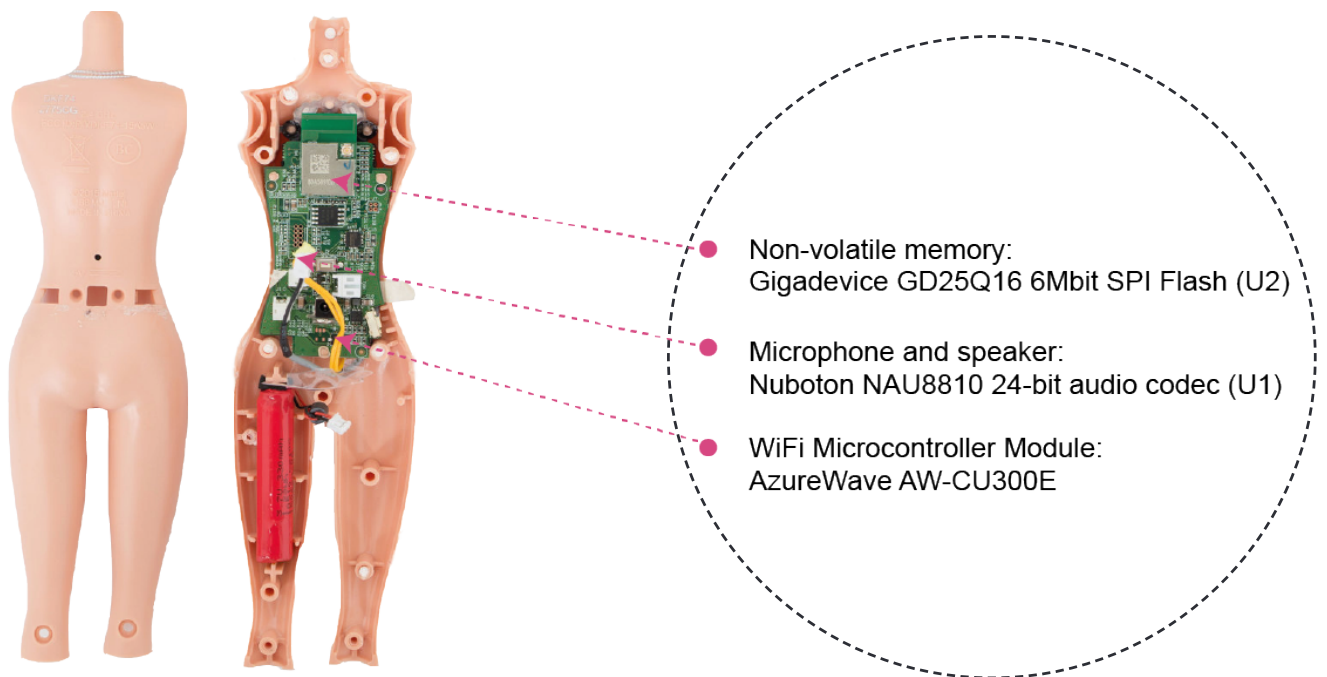
Toys like this also raise questions about the appropriate support and guidance necessary for toy manufacturers who understand much about conventional issues relating to toy safety standards but have little or no expertise in data protection law. The market for IoCT toys is expected to double to US$18b by 2023 (Juniper-Research, 2018). However, whether these toys will bring joy to children or endanger their safety, security, and privacy in unprecedented ways with implications for their physical and mental health will depend on raising global standards to follow a common set of implementable and agreed standards.

A   Smart toys are devices that use artificial intelligence. However smart toys must also be connected to the internet to be an IoT. Here we focus on consumer IoT devices and for the purposes of this report, IoCT devices do not include consumer IoT devices for adults but sometimes used by children.

Device level vulnerability: easy to hack

As IoT technology evolves and hacking gains in sophistication, the challenge for cybersecurity to remain ahead of the risks is inevitably a technological one to some extent. When the *Hello Barbie* doll was launched, it was rated by security experts as "the most security and privacy hardened toy of its kind" with data encryption and "secure tunnels protected at each end by cryptographic protocols and digital certificates intended to make sure that even if a child's conversation is intercepted, the data will be gibberish to eavesdroppers" (Sposito, 2015). Nevertheless, security experts had soon found basic design flaws; from an easily hackable ID, connectivity to any "Wi-Fi network with "Barbie" in its name", to being exposed to the 'Poodle' vulnerability (Coldewey, 2015). Likewise, critical security flaws were found in a 2017 study of children's smart watches by the Norwegian Consumer Council (Norwegian-Consumer-Council, 2017, pp. 3–4). Thus, more than the technological challenge of staying ahead of hackers, what is salient here are the challenges to the implementation of basic security features in IoCT manufacturing like basic authentication and encryption (Chu, Apthorpe, & Feamster, 2018; Jones & Meurer, 2016; Norwegian-Consumer-Council, 2017), that endanger children's safety and security.

- Non-volatile memory:
  Gigadevice GD25Q16 6Mbit SPI Flash (U2)

- Microphone and speaker:
  Nuboton NAU8810 24-bit audio codec (U1)

- WiFi Microcontroller Module:
  AzureWave AW-CU300E

Figure 10: Easy to unpack, easy to hack?
Hello Barbie Security Teardown. Image adapted from Somerset Recon. View their security analysis here.

However, implementation of secure manufacturing is a complex process. It requires substantial knowledge of the rapidly evolving cyber threat and security landscape to be efficacious. This knowledge, or the capital and skilled resources needed to acquire and implement this knowledge, is either unavailable or out of reach for most of the small and medium sized toy manufacturers who represent the bulk of the supply-side in the global IoCT sector (99% of Europe's toy sector are SMEs, of which 88% are micro-enterprises (BTHA in BrandonGaille, 2018)). While these SMEs have built up expertise and knowledge in other safety issues relevant to toys, such as the size of small parts for age appropriate toys, safe materials to use, risks with toys coming apart etc., they may know much less about cybersecurity, data protection, or the salience of secure manufacturing.

In a highly competitive and fast moving market, some toy manufacturers are releasing connected toys without adequate safety and security features. On one hand, this is a competitive and dynamic marketplace where first movers are rewarded. In addition, the skillset and knowledge base of conventional toy safety is mismatched to these new toys and addressing that divergence will require investment and new learning – especially challenging for SMEs. Secure software development and cybersecurity are very novel demands on the sector and there will be a cost to incorporating them. However, the fact remains that these toy manufacturers are placing consumer safety and privacy at risk. Whether this occurs due to the immaturity of the sector, due to market pressures, or through a lack of sectoral attention to the problem is not clear. However, there are no indications that this will be addressed through market forces. Instead, the certainty of legislation to maintain standards would level the playing field and make clear for SMEs where they need to invest to make their toys market ready.

Network level vulnerability: lack of privacy
In addition to the risks to consumers of engaging with the devices themselves, the interconnectedness of IoCT devices mean that poorly secured devices offer a potential soft entry-point for cybercriminals to gain unauthorised access to wider networks, including allowing intruders to gain access to home or institutional networks. A survey of workplace wi-fi networks by *OpenDNS* found that the more mundane devices such as children's *LeapFrog* laptops were particularly likely targets. Equipped with a simple Bluetooth connectivity that showed up on workplace networks, these devices were often overlooked by IT staff but introduced vulnerabilities to all connected networks including access to critical infrastructure (Sposito, 2015). Beyond introducing infrastructural vulnerabilities, what is more concerning is the increasing ease with which IoCT devices can connect to other devices using ubiquitous short-range communications technologies such as wi-fi, bluetooth or zigbee. This places children's privacy,

safety, security and, ultimately, development at risk. As a survey of IoCT devices by the UK-based consumer rights group *Which?* revealed:

> it makes it "far too easy for someone to illicitly pair their own device to the toys and use the tech to talk to a child. ...[One] would need hardly any technical know-how to 'hack' [a] child's toy" (Laughlin, 2017).

Moreover, the notion that the massive amounts of data collected from various IoT devices ('Big Data'), including data on children's whereabouts and behaviours, are anonymised and stored in data clouds inextricably delinked from its source, is misleading. Recent studies reveal that digital "fingerprints" left by IoT devices make re-identification of anonymised sensor data (i.e., data with personally identifiable information such as name, address, telephone number removed) much easier than previously thought (Hardesty, 2013; Nikander, Siegel, & Viitala, 2020; Zhang et al., 2019). However, this is yet to be addressed in privacy law (Peppet, 2016; Sun et al., 2020).

These questions become even more urgent given the influx of IoCT devices from various jurisdictions including from those with much lower, if any, standards of data protection and consumer rights. In particular, flooding of markets with IoCT devices manufactured in overseas markets like China with lower security standards or less rigorous privacy policies for data collected is a growing concern for regulators. This is primarily because the sheer volume of products far outstrip monitoring (and oversight) resources (see e.g., children's smart watches in Norwegian-Consumer-Council, 2017, p. 3) (see also Weisskopf, 2007). This is exacerbated if local manufacturers buy or copy toy plans from these markets – thereby replicating the weaknesses embedded within them.

Despite a growing understanding of the range of privacy and security risks inherent in IoT devices in general, and IoCT devices in particular, ethical, legal, and social implications differ across sectors and require careful consideration in the design and delivery of secure manufacturing and policy initiatives. This is especially the case for assuring children's safety and security as discussed below.

IoCT vulnerabilities: implications for children

Children's Right to Privacy

Critical security flaws in the design of IoCT devices combined with the privacy issues of interconnectedness critically challenge children's (and their family's) right to privacy. The extent of this privacy challenge is perhaps best demonstrated by the *Cloudpets* experience. In early 2017, users of the connected *Cloudpets* range of toys discovered their database exposed online. Private security researcher, Troy Hunt explained that the breach revealed:

> references to almost 2.2 million voice recordings of parents and their children exposed by databases that should never have contained production data …[which had been left] exposed publicly to the web without so much as a password to protect it or any encryption. The services sitting on top of the exposed database [were] able to point to the precise location of the profile pictures and voice recordings of children (Hunt, 2017)

Of course, the scale of this privacy violation is deeply concerning. Equally alarming is the extent of the vulnerability. Security researchers found that it was "possible to access the voice recordings without any authentication if [one had] the exact URL at which they are stored – something that can be gleaned by examining the app when a user is logged in" (Hern, 2017). This, more than anything, emphasised the extent of the knowledge gap at the manufacturer Spiral Toys (Hern, 2017; Lomas,

Figure 11: Cloudpets: cute and cuddly?
CloudPets Security Teardown. Image adapted from Cure53.

Figure 12: Digital Shadow: reselling 'used' Cloudpets
Source: ebay.co.uk; accessed on 24 November 2020

2017a). Essentially though, as a consequence of this one breach alone, the private conversations of potentially millions of children have been compromised.

There are further problems with data security when an IoCT device manufacturer goes into administration, is taken over by another firm, or ownership (or management) changes. Within this context, privacy challenges are exacerbated as the data generated by the IoCT, including children's private conversations and behavioural data, becomes accessible to new third parties. The provenance of this sensitive data is not always handled appropriately and guidance or rules on how to do so is urgently required.

This is also the case with every subsequent re-sale of 'used' IoCT devices; previously collected data can be easily accessed by new owners and follows the toy like a *Digital Shadow* (BBC, 2018; Seals, 2018). Indeed, 'used' *Cloudpets* continued to be re-sold in online marketplaces long after its manufacturer Spiral Toys was dissolved in 2017 (see Figure 12). This greatly confuses who or how many third-parties have access to the data collected, the (il) legal basis on which this data is shared, by whom, and to what purpose (see e.g., detailed discussion on user's *right to data portability* in Turner et al., 2020; and *informed consent* in Tanczer et al, 2017). A concerning response from IoT toy manufacturers has been to shift responsibility for data and privacy protection on to consumers (parents) through various legal such as 'opt-in/opt-out' policies (Holloway & Green, 2016, p. 2). How society treats these privacy challenges, whether we distance ourselves from them, normalise them, or act to prevent them, has consequences for children's safety (Vallejo, Muñoz, &

Hernando Rosales, 2018), security (Doyle & Veranas, 2014), autonomy (Ghosh et al, 2018) and development (Duerager & Livingstone, 2012; Littman, 2011; Turner, 2020).

Children's autonomy: parental surveillance

IoT toys like *Hello Barbie*, *CloudPets,* and *My Friend Cayla* raise questions over the extent of parental (and non-familial or external) surveillance and its implications for children's autonomy and their development. Scholar of data and society, Helena Nissenbaum (2004) has argued that information gathering and dissemination should be appropriate to each context and respect the governing norms within it. However, norms and laws around online privacy center on issues of public surveillance and become blurred when it comes to parental surveillance. If public surveillance "constitutes injustice and even tyranny …[when] it violates a right to privacy because it violates contextual integrity" (Nissenbaum, 2004, p. 119) especially "when the parties involved are of radically unequal power and wealth" (ibid, p. 157), then the subjective and contingent complexity of the parent-child relational context blurs a clear interpretation of what parental surveillance *should be*.

Parents (as adults, nurturers, and carers) undeniably hold power over children. However, this power is typically mediated through 'reciprocity' and 'power-sharing' parent-child relationships founded on mutual trust and trustworthiness that crucially shape children's development (Nissenbaum, 2004; Russell et al., 1998). Parental surveillance, especially "covert monitoring if discovered" (Rotenberg, 2010) erodes mutual trust (Livingstone, 2008). This is not only harmful for children's development but can also endanger their safety as surveilled children are less likely to confide unsafe behaviour to parents (Kramer, 1999; Smetna, 2010; in Mathiesen, 2013). Instead, a balanced approach to parental supervision between "the duty to nurture with the duty to respect the rights of the child [children's autonomy]" is recommended (Brennan & Noggle, 1997, p. 8).

Nevertheless, a clear understanding of how much supervision is too much (to be considered 'unjust' or 'tyrannical' surveillance harmful for a child's autonomy and development) is highly subjective and dependent on individual family circumstances and each child's needs (Coley & Hoffman, 1996; Crouter & Head, 2002). Thus, many suggest open discussions between parents and children about safe online behaviour [30-32], (Duerager & Livingstone, 2012; Kirwil, 2009; Littman, 2011), greater involvement of children in the design of 'online safety' features (Ghosh et al., 2018), legislative support for parent's efforts in tackling the rapidly evolving nature of online privacy concerns (Livingstone & Bober, 2006) and support (including rehabilitation arrangements) of children known to social services.

Children's autonomy: non-familial surveillance

Legislation is especially recommended for IoCT devices that bring non-familial (external) surveillance into children's private spaces in unprecedented ways for mostly unknown purposes by unknown third-parties (Livingstone & Bober, 2006). The combination of embedded surveillance tools such as cameras, microphones, sensors with internet connectivity transmitting data to multiple data processing companies (for facial recognition, voice detection, machine learning, data analytics etc.) create a concerning set of conditions for non-familial surveillance to thrive. In 2017, Germany's regulator *Bundesnetzagentur* (2017) banned the *My Friend Cayla* IoT doll for having a "concealed surveillance device," ordering parents to 'destroy' the toy or face hefty fines. A key concern noted by *Bundesnetzagentur* was that the *Cayla* doll could,

> record and transmit anything a child says without their parents' knowledge....[while any] company could also use the toy to advertise directly to the child or the parents" (Walsh, 2017).

Thus in this sense, accepting "...that it's OK to have their trusted best friend spying on them or recording their every word" (Claire Gartland, Director, Consumer Privacy Project, Electronic Privacy Information Center (EPIC) in (Picchi, 2016) represents a normalisation of a non-familial and unknown external authority in a child's development that turns children into 'governable subjects' (Foucault, 1977 in Pinto & Nemorin, 2014). Drawing on the example of the non-IoT Christmas toy '*Elf on the Shelf*' and its popularity among (grand)parents for influencing 'naughty' children's behaviour to become 'nice' (see Figure 13), Pinto & Nemorin

The Elf on the Shelf asks children to "adopt a scout elf" that "reports to Santa Claus each night to let him know who has been naughty or nice".

"After arriving on the first night, George [customer's nickname for the Elf] began his mission to spy on our daughter and ensure the big Jolly guy had the information he needed to determine if our daughter was naughty or nice... I personally believe this was a way of testing our daughter to see which side of the list she would be on. Luckily, our daughter seemed to have passed these tests with flying colors..."

Parent - December 2015

"Kids Went From Naughty List to Nice List: I ordered this for my grandkids who were in danger of being put on the naughty list. ...The kids started going to bed without a fuss, and one even woke up early and started cleaning her room without being asked! With their Elf partners help, they stayed on the nice list..."

Grandparent - February 2016

Figure 13: Evolving modes of surveillance: naughty or nice? *(Reviews of 'Elf on the Shelf' on Amazon.com)*

asked if it was acceptable to "prepar[e] a generation of children to accept, not question, increasingly intrusive (albeit whimsically packaged) modes of surveillance?" (ibid). For these evolving modes of surveillance and monitoring, especially as more IoT-based toys becomes available, are not value-free (Nissenbaum, 2001) and critical awareness of (what or whose) values these toys represent and whether they are desirable for the safe development of children is needed before contemplating their normalisation in society.

Alongside these more visible and widely discussed issues of familial and non-familial (external) surveillance, research is also emerging on the psychological implications of rapidly evolving IoT-mediated surveillance technologies on children (Lomas, 2017b; PsycholoGenie., n.d.). One strand of emerging research centres on the psychological implications of artificial intelligence (AI) enabled anthropomorphism in IoT toys. Anthropomorphism is the attribution of human characteristics to non-human objects and animals. However, Google's 2012 patent for an anthropomorphic IoT teddy bear (see Figure 14) raised considerable concerns around the psychological implications on children alongside safety and security
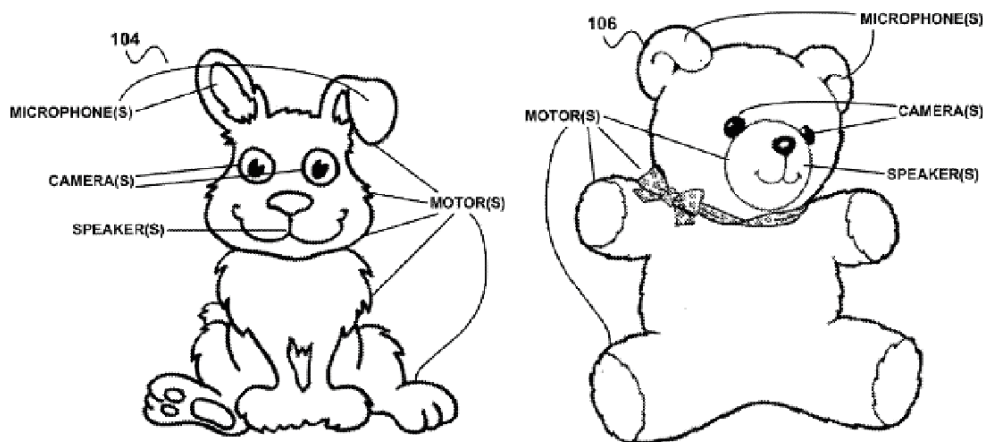
[0076] To express interest, an anthropomorphic device
may open its eyes, lift its head, and/or focus its
gaze on the user or object of its interest. To express
curiosity, an anthropomorphic device may tilt its head,
furrow its brow, and/or scratch its head with an arm. To
express boredom, an anthropomorphic device may defocus
its gaze, direct its gaze in a downward fashion, tap its
foot, and/or close its eyes. To express surprise, an
anthropomorphic device may make a sudden movement, sit or
stand up straight, and/or dilate its pupils. However, an
anthropomorphic device may use other non-verbal movements
to simulate these or other emotions.

Figure 14: "Visions of an IoT Chucky". Patent #: US 2015/0138333 A1 'Agent interfaces for interactive electronics that support social cues', Google Inc., Mountain View, CA (US)

issues (Kelion, 2015; Storm, 2015). UNICEF has also written about the ways in which the increasingly prevalent but little discussed practices such as "always-on surveillance …that continuously monitor everything from children's engagement in the classroom to their emotional states throughout the day threaten the creativity, freedom of choice and self-determination of children…" (UNICEF, 2019).

Child Sexual Abuse
Internet-mediated children's abuse from **online solicitation** (Crowell et al., 2020) and grooming for **sexual exploitation** (Kloess, Beech, & Harkins, 2014; Medvedeva & Dozortseva, 2019; Nikolovska, 2020), **mental abuse** (Chiang & Grant, 2019) including **cyberbullying** (Gámez-Guadix & Mateos-Pérez, 2019; TheGuardian, 2015) and the production and dissemination of **child sexual abuse imagery** (Babchishin, Hanson, & VanZuylen, 2015; Gillespie, 2010) have risen exponentially over the past two decades (Merdian et al., 2019; Stanley, 2001; Wallace, 2020).

Most of this online abuse is mediated via computers or smartphones (Wallace, 2020). Few, if any such instances of abuse are perpetrated via IoCT devices such as kids smartwatches, toys etc. mainly because IoCT devices typically offer limited scope for browsing online despite being connected to the internet, unlike computers and smartphones. For instance, *Facebook* alone accounted for nearly 12 million online child sexual abuse images (The Guardian, 2015; Keller & Dance, 2019) but cannot **yet** be browsed on IoCT devices. Only one study, by the *Internet Watch Foundation* in 2014, has so far linked child sexual abuse to IoCT devices; finding that poorly secured (or unsecured) IoT devices were likely to be targeted by paedophiles using short-range bluetooth or wi-fi connectivity to scout for 'safe spaces' to stash child abuse imagery (Morley, 2016).

Bullying and Psychological Abuse of Children
A handful of studies have also linked IoCT toys to bullying or psychological abuse of children. One study found that attackers could manipulate children's behaviour using 'audio injection' in children's trusted IoT toys by commanding children to, for example,

> open the door to their houses, or to change combination locks, or tell lies about their parents. The attacker can even be mean to the child, insulting their appearance or intelligence and therefore eroding from an early age their self-esteem and their trust of the toy and technology" (Valente & Cardenas, 2017)

While studies do not explicitly provide known instances of bullying or psychological abuse perpetrated via IoCT

devices[B], the possibility that this might happen is a growing concern e.g., as revealed by a 2017 public service announcement issued by the US Federal Bureau of Investigation warning parents against:

> the potential misuse of sensitive data [in IoT toys] such as GPS location information, visual identifiers from pictures or videos, and known interests to garner trust from a child could present exploitation risks" (FBI, 2017)

These risks are heightened by evolving methods of 'data exfiltration' (TheGuardian, 2015) whereby attackers steal sensitive images collected by IoCTs and various evolving forms of 'tech abuse' targeting minors especially during the recent lockdown (please see detailed discussion of 'IoT facilitated tech abuse' earlier in Section 2, Issue 1).

What is being done

In the UK and US, an industry self-regulatory approach is used to ensure cybersecurity in the IoCT sector. **In the UK**, 'toy' manufacturers and distributors are predominantly represented by the *British Toy & Hobby Association* (BTHA) which has been at the forefront of the toy industry's efforts (calling on its member manufacturers) to adopt the UK CoP guidelines for secure manufacturing in existing toy manufacturing processes (BTHA, 2019). The BTHA goes further to acknowledge the paucity of security expertise available to toy manufacturers (discussed earlier) and recommends members engage with cybersecurity expertise at the Open Web Application Security Project (OWASP) to identify and address security risks in their manufacturing practices (ibid). A similar level of proactive engagement with cybersecurity and privacy has yet to emerge amongst other industry groups representing more niche interests such as the *Association of Play Industries* (API), *Baby Products Association* (BPA), *Equitoy* (formerly the *British Toy Importers Association*), the *Toy Retailers Association* (TRA).

In the US, state agencies are held responsible for their own cybersecurity according to the Federal Information Security Modernization Act (FISMA) in compliance with the "security baselines mandated" by the Federal Acquisition Regulation (FAR) for "federally procured IoT devices" (Crawford & Sherman, 2018). Otherwise, self-regulation prevails in the private sector led by a patchwork of industry-led associations with stated 'cybersecurity' mission statements. However, tensions exist between this mission and the trade or industry association's typical mandate for bringing more products to market.

B   It is unclear if this is due to privacy protection and media reporting laws in crimes involving children or absence of real world instances.

Meanwhile, resource-strapped federal agencies such as the US' *Consumer Products Safety Commission* (CPSC) (which regulates the US toy market) rely on highly resourced industry associations to bridge resource gaps in their underfunded departments. However, it is argued that this proximity typically yields vital policy-shaping influence to consortia members whose interests may not always align with the delivery of public good (Weisskopf, 2007). Notwithstanding, resources provided by industry and non-governmental actors add valuable capacity to government oversight efforts.

However, a lack of meaningful coordination across these multiple stakeholders challenge efforts towards developing an effective regime of implementable standards and norms for IoCT security and safety (Chu et al., 2018; Crawford & Sherman, 2018). Intra-governmental fragmentation adds a further layer of complexity when implementing and standardising cybersecurity across all consumer IoT domains whether for a medical purpose, a toy or a vehicle (Brass et al., 2018; Tanczer, et al., 2019). Currently, cybersecurity and privacy for **IoT medical devices are governed by health regulators** (e.g., USFDA, UKMHRA, Japan's PMDA, EMA), for **IoT vehicles by transport authorities** (e.g., the US *National Highway Traffic Safety Administration* (NHTSA), the UK's *Centre for Connected and Autonomous Vehicles* (CCAV), for **IoT toys by product safety agencies** (e.g., UK's *Office for Product Safety & Standards*, US' *Consumer Products Safety Commission* (CPSC).

The few instances in which stakeholders across government departments and non-state actors have worked together provide a powerful example of what it will take to secure children's futures. In 2016, **one public agency** (*The US Federal Trade Commission*) and **several consumer rights organisations** *(The Electronic Privacy Information Center*, *The Campaign for a Commercial Free Childhood*, *The Center for Digital Democracy*, and *Consumers Union)* came together to successfully ensure children's right to privacy in a legal case against Genesis Toys (EPIC-FTC, 2016)[c].

In reality, multistakeholder coordination including consensus within various intra-governmental departments and agencies (each with discreet mandates for provisioning specific services for different sectors) is a complex political and administrative process. Secure manufacturing protocols applicable to consumer IoT manufacturing across all sectors, if standardised, would not only provide the foundational basis for assuring public safety and security in IoCT devices, but would also allow vital multistakeholder resources to instead extend and strengthen these 'base' standards.

---

c   Manufacturer of the IoT toys My Friend Cayla and i-Que Intelligent Robot.

Conclusion

"Despite their potentially serious impact, [IoCT] vulnerabilities are all easily correctable" say experts at Princeton University's Computer Science Department (Chu et al., 2018, p. 1). Their findings not only revealed several design and configuration flaws in the IoT toys they studied but also how these flaws violated both the "US Federal Trade Commission's Children's Online Privacy Protection Rule] COPPA" as well as promises made in the manufacturers own privacy policies (ibid). While vulnerabilities are indeed correctable, the road to that destination as we have shown here, is likely to be neither easy nor quick, whether from the perspective of SME manufacturer's capacity, their understanding of the profound implications (of privacy, security, and security) or the multistakeholder coordination needed.

Small and medium manufacturers that make up the bulk of the IoCT manufacturing space (The British Toy and Hobby Association (BTHA) in BrandonGaille, 2018) will require support and guidance to understand, identify, and translate the rapidly evolving cybersecurity and cyberthreat landscape into effective business tools before considering a transition to secure manufacturing practices. While some of the support and guidance will invariably need to come from the IoCT industry's own initiatives, state support (whether legislative or economic) will be crucial to its sustainability and success although garnering it is likely to be complex and long-term process (Carr & Tanczer, 2018). Here, standardisation of key implementable security protocols can help by crucially bringing together the currently fragmented governance space under a unified, coherent, and enforceable mechanism that utilises existing knowledge to ensure secure manufacturing (Brass & Sowell,(Brass & Sowell, 2020; Lee, 2019). Towards this end, legislating and enforcing the basic standards of IoT security such as no default password, vulnerability disclosure etc., recommended by the UK DCMS, will be a first step towards standardising secure manufacturing across all IoT domains (health, transport, toys etc.) before eventually placing upward pressure on global standards.

Section 2
UK Code of Practice for
Consumer IoT Security:
'Where we are'

Introduction

It is not always immediately clear how a guidance document like the UK CoP is taken up across global industry and policy communities. In this section, we present our findings from an exercise in which we traced the UK CoP's journey from guidelines to its contribution (alongside the significant contribution of various stakeholders) to the development of TS 103 645 in February 2019 and the development of ETSI EN 303 645 in June 2020.

A data-mining approach is used to extract Google results for keywords and variations of keywords related to CoP, the TS 103 645 and the EN 303 645 (see detailed discussion of methods in Annex 1). A co-occurrence network is created by mapping keywords that occur together in a document (see detailed discussion of methodology in Annex 1). A visualisation of the interrelationships between keywords and between the first three UK CoP guidelines, namely 'default password', 'vulnerability disclosure' and 'software update' is also provided.

It remains to be seen whether the development of the UK CoP and the subsequent development of the ETSI EN 303 645 will push manufacturers serving the European market towards adopting secure manufacturing. If it does, it could well drive up IoT safety and security standards elsewhere - especially in those countries with a higher number of manufacturers that serve the EU market.

The UK Government's Code of Practice for Consumer Internet of Things Security (UK CoP for CIoTS) to European Telecommunications Standards Institute (ETSI) EN 303 645.

March 2018	February 2019	June 2020

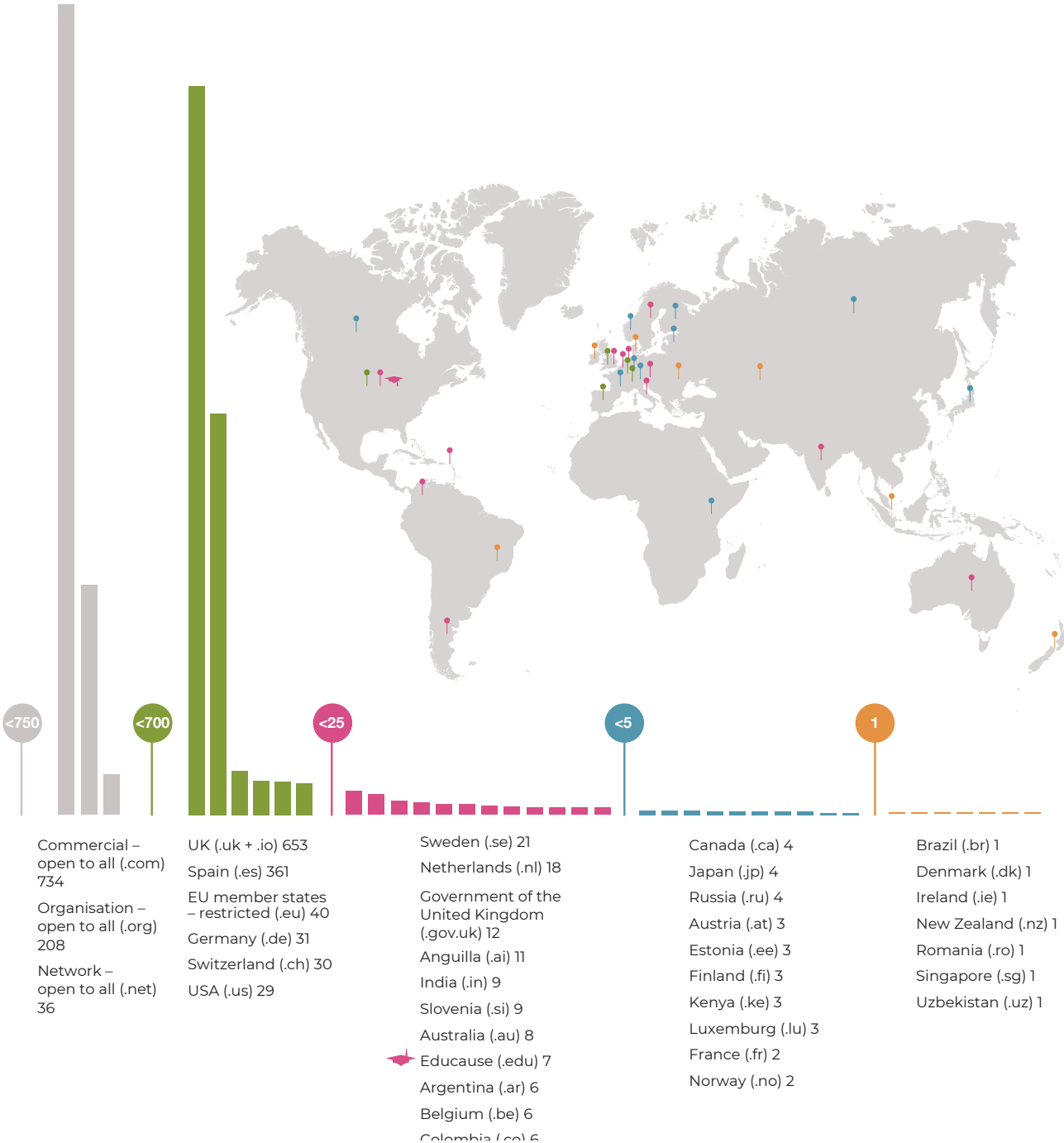| UK CoP	TS 103 645	EN 303 645

The Code of Practice brings together, in thirteen outcome-focused guidelines, what is widely considered good practice in IoT security. It has been developed by the Department for Digital, Culture, Media and Sport (DCMS), in conjunction with the National Cyber Security Centre (NCSC), and follows engagement with industry, consumer associations and academia. The Code was first published in draft in March 2018 as part of the

In February 2019, ETSI, the European Standards Organisation, launched the first globally-applicable industry standard on internet-connected consumer devices. ETSI Technical Specification 103 645 brings together what is widely considered good practice in consumer IoT security.

ETSI European Standard 303 645 published in June 2020 establishes a security baseline for Internet-connected consumer devices and provides a basis for future Internet of Things product certification schemes. Many organisations have already based their products and certification schemes around the EN and its predecessor TS.

Global uptake of CoP*

* By DNS of websites that mention UK CoP, TS 103 645 or EN 303 645. Please see discussion of methods in Annex 1

<750

Commercial – open to all (.com) 734

Organisation – open to all (.org) 208

Network – open to all (.net) 36

<700

UK (.uk + .io) 653

Spain (.es) 361

EU member states – restricted (.eu) 40

Germany (.de) 31

Switzerland (.ch) 30

USA (.us) 29

<25

Sweden (.se) 21

Netherlands (.nl) 18

Government of the United Kingdom (.gov.uk) 12

Anguilla (.ai) 11

India (.in) 9

Slovenia (.si) 9

Australia (.au) 8

Educause (.edu) 7

Argentina (.ar) 6

Belgium (.be) 6

Colombia (.co) 6

<5

Canada (.ca) 4

Japan (.jp) 4

Russia (.ru) 4

Austria (.at) 3

Estonia (.ee) 3

Finland (.fi) 3

Kenya (.ke) 3

Luxemburg (.lu) 3

France (.fr) 2

Norway (.no) 2

1

Brazil (.br) 1

Denmark (.dk) 1

Ireland (.ie) 1

New Zealand (.nz) 1

Romania (.ro) 1

Singapore (.sg) 1

Uzbekistan (.uz) 1

National and global reach of keywords

Keyword	% of mentions	National Reach	Global Reach
🔍 www	✓		
UK IoT Policy	29.72%	8.84%	8.82%
Default Password	5.04%	0.25%	0.25%
ETSI	3.99%	0.16%	0.16%
TS Standards	1.86%	0.03%	0.03%
Software Update	3.18%	0.10%	0.10%
UK CoP IoT	43.68%	19.08%	19.04%
Vulnerability Disclosure	4.47%	0.20%	0.20%
IoT	52.43%	21.04%	20.88%

Interrelationships of the UK CoP with ETSI standards and basic guidelines*

* by co-occurence of keywords (circles); thicker line represents strength of co-occurence. Please see discussion of methods in Annex 1

- IoT
- UK Code of Practice
- IoT ETSI
- IoT Policy
- TS Standards

Guidelines:

- Default Password
- Software Update
- Vulnerability Disclosure
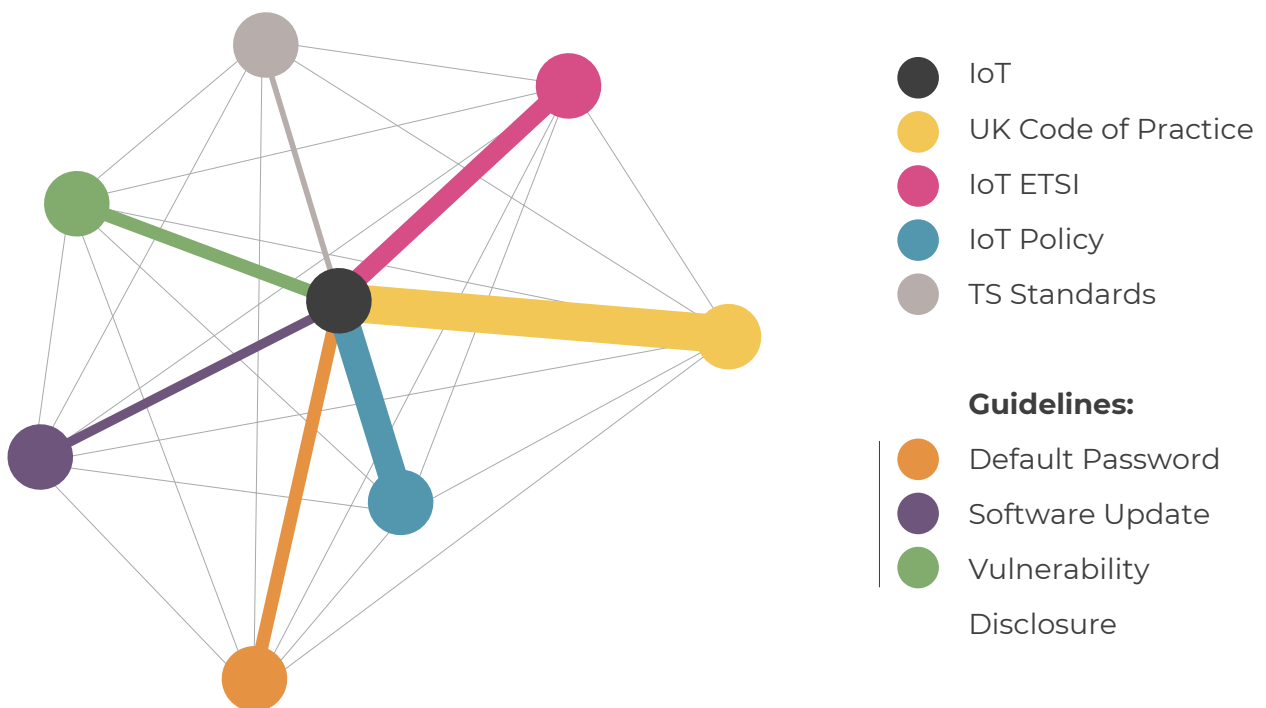
Annex 1
Methods

Methods

We use a 5-step process for crawling, scraping, cleaning, mapping and visualising the co-occurrence of keywords fto help in determining the uptake of the CoP.

A web crawler or a "spider" was used to search Google using the keywords – here we make use of the APIFY tool that returns the Google Search Result Pages (SERPs), and data is output in the HTML or CSV format. We use 8 Keywords and 26 variations of these keywords. Through the combination of the 26-keyword variation (see below), we obtained a total of 2279 results (unique websites) containing the Keyword term used to search the Google API (Application Programming Interface), the name of the organisation, the title of the document, document date, the URL of the document, the frequency of the keyword that is found in the document and the phrase where the keyword is present are extracted (where available).

In the second step, the information is retrieved using the process of web scrapping. We use Python's Beautiful soup library to parse the results from the APIFY Google SERP crawler and to extract data.

In the third step, we cleanse the data and check for consistency after merging results from the first two steps. Data frames that hold incomplete information are removed in this step. The fourth step involves extracting data to create the network. Here a bipartite network is created based on the keyword search and the website that reference the keyword. The bipartite network is then projected to a one-mode keyword co-occurrence network.

The final stage in this process is knowledge discovery. Network analysis is conducted to understand the most cited keywords and the reach of the keywords both at national and international levels using Degree and Eigenvector's network centrality measures (please see Vasudevan et al, Under Review in Scientometrics).

Keywords decided with User Partner 1 (DCMS) and used for the search strategy

Level	Keyword (search string)	Keyword variations
Level 1	UK CoP Consumer IOT	UK CoP Consumer IOT
		UK CoP IOT
		UK Code of Practice Consumer IOT
		UK CoP Consumer Internet of Things
		UK CoP Internet of Things
	DCMS IOT	DCMS IOT
		DCMS Internet of Things
		DCMS Internet of Things Policy
		DCMS IOT Policy
		DCMS Policy
		DCMS Consumer IOT
		DCMS Consumer IOT Policy
	UK IOT	UK IOT
		UK Internet of Things
		UK IOT Policy
		UK Internet of things Policy
		IOT Policy UK
	UK DCMS IOT	UK DCMS IOT
Level 2 by organisations	ETSI EN	ETSI EN 303 645
		EN 303 645
		TS 303 645
		TS 103 645
Level 3 by guidelines	No Default Password	Default Password
	Vulnerability Disclosure	Coordinated Vulnerability Disclosure
	Keep Software Updated	Keeping software updated

Step 1	Step 2	Step 3	Step 4	Step 5
Information Identification	**Information Retrieval**	**Information Cleansing**	**Relationship Extraction**	**Knowledge Discovery**
Step 1: Use APIFY web crawler to search for 8 keywords and 26 variations. Keywords include: • UK CoP Consumer • IoT • DCMS IoT • UK IoT • UK DCMS IoT • ETSI EN • Default Password • Vulnerability Disclosure • Keep Software Updated **Step 2:** Set the results to 100 search results per keyword **Step 3:** Language restricted to English language documents **Step 4:** Use organic results only	**Step 1:** Use the Beautiful Soup library of Python **Step 2:** Use the results from APIFY SERP to mine data from each of the identified links for: • Organisation Name • Title of the document • Publication Date • Keyword count • Phrases used from the initial search string Additional search based on "what others search for" in Google also mined in this step to obtain frequency count of substrings used in each of the search results	**Step 1:** Merge all results from the previous stages **Step 2:** Check for information consistency: • Remove duplicates • Remove records that have unidentified character sets • Remove Twitter records • Data removed is less than 5% threshold - manual intervention not necessary	**Step 1:** Create a bipartite network with the document title and keyword **Step 2:** Using the threshold of at least 1, the bipartite network is projected using sum-of-cross-productes method. This captures the overlap between the pair of document/keywords by summing the multiplied elements of the corresponding rows/columns of the adjacency matrix	**Step 1:** Using the weighted square matrix of keyword co-occurrence, calculate the degree and eigenvector centrality to identify the local and global network reach of keywords

References

Adhikari, R. (2015). Talking Barbie Says Hello, Parents Say Goodbye. TechNewsWorld. (March 18). Retrieved from https://www.technewsworld.com/story/81837.html

Alsuwaidi, A., Hassan, A., Alkhatri, F., Ali, H., & Mohammad, Q. H., Alrabaee, S. (2020). Security Vulnerabilities Detected in Medical Devices. IEEE. 2020 12th Annual Undergraduate Research Conference on Applied Computing (URC): pp. 1-6.

Arora, S., Yttri, J., & Nilsen, W. (. (2014). Privacy and security in mobile health (mHealth) research. Alcohol research: current reviews 36(1): 143.

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. Computer Networks 54(15): 2787– 2805.

Babchishin, K. M., Hanson, R. K., & VanZuylen, H. (2015). Online child pornography offenders are different: A meta-analysis of the characteristics of online and offline sex offenders against children. Archives of Sexual Behavior, 44: 45-66.

BBC. (2017). NHS "could have prevented" WannaCry ransomware attack. BBC News. (October, 27). Retrieved from https://www.bbc.co.uk/news/technology-41753022

BBC. (2018). Amazon and eBay pull CloudPets smart toys from sale. (June, 6). British Broadcasting Corporation. Retrieved from https://www.bbc.co.uk/news/technology-44382135

Bellini, R., Forrest, S., Westmarland, N., Jackson, D., & J. D. Smeddinck. (2020). "Choice-Point: Fostering Awareness and Choice with Perpetrators in Domestic Violence Interventions," in Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, Honolulu HI USA.

Bellini, R., Strohmayer, A., Olivier, P., & C. Crivellaro. (2019). "Mapping the Margins: Navigating the Ecologies of Domestic Violence Service Provision," in Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems - CHI '19, Glasgow, Scotland UK.

Bernabeu, G. (2019). The EU Cybersecurity Act: What is it and what does it mean for Europe? (11 July). Retrieved from https://www.vanillaplus.com/2019/07/11/47576-eu-cybersecurity-act-mean-europe/

Best, J. (2018). Smart watches, fitness trackers and the NHS: Are wearables just what the doctor ordered? (November, 21). ZDnet. Retrieved from https://www.zdnet.com/article/smart-watches-fitness-trackers-and-the-nhs-are-wearables-just-what-the-doctor/

Blythe, J., & Lefevre, C. (2016). How to save the Internet of Things from cyber attacks – with psychology. The Conversation, (November, 14). Retrieved from https://theconversation.com/how-to-save-the-internet-of-things-from-cyber-attacks-with-psychology-68608

BrandonGaille. (2018). 19 UK Toy Industry Statistics and Trends. Brandon Gaille Small Business and Marketing Advice. (November, 10). Retrieved from https://brandongaille.com/19-uk-toy-industry-statistics-and-trends/

Brass, I., & Sowell, J. H. (2020). Adaptive governance for the Internet of Things: Coping with emerging security risks. Regulation & Governance.

Brass, I., Tanczer, L., Carr, M., Elsden, M., & Blackstock, J. (2018). Standardising a Moving Target : The Development and Evolution of IoT Security Standards. IET, 1–9. Retrieved from https://digital-library.theiet.org/content/conferences/10.1049/cp.2018.0024

Brennan, S., & Noggle, R. (1997). The moral status of children: Children's rights, parents' rights, and family justice. Social Theory and Practice 23: 1–26.

BTHA. (2019). Connected toys and the Internet of Things. The British Toy and Hobby Association. Retrieved from https://www.btha.co.uk/wp-content/uploads/2019/11/BTHA-IoT-connected-toys-article-publish.pdf

Bundesnetzagentur. (2017). Bundesnetzagentur zieht Kinderpuppe "Cayla" aus dem Verkehr. (Federal Network Agency pulls children's doll "Cayla" out of circulation). (February 17).

CBSNews. (2018). How medical devices like pacemakers and insulin pumps can be hacked. CBS News. (November, 8). Retrieved from https://www.cbsnews.com/news/cybersecurity-researchers-show-medical-devices-hacking-vulnerabilities/

Chatterjee, R., & et al. (2018). "The Spyware Used in Intimate Partner Violence," in 2018 IEEE Symposium on Security and Privacy (SP), pp. 993–1010.

Chiang, E., & Grant, T. (2019). Deceptive identity performance: Offender moves and multiple identities in online child abuse conversations. Applied Linguistics, 40(4): 675-698.

Ching, K. W., & Singh, M. M. (2016). Wearable technology devices security and privacy vulnerability analysis. International Journal of Network Security & Its Applications 8(3): 19-30.

Chu, G., Apthorpe, N., & Feamster, N. (2018). Security and privacy analyses of internet of things children's Toys. IEEE Internet of Things Journal 5(1) https://doi.org/10.1109/JIOT.2018.2866423.

Citron, D. (2009). "Law's expressive value in combating cyber gender harassment," Michigan law review, vol. 108, pp. 373–416.

Citron, D., & Franks, M. A. (2014). "Criminalising revenge porn," Wake Forest Law Review, vol. 49, pp. 345–391.

Clark, G. W., Doran, M. V., & Andel, T. R. (2017). Cybersecurity issues in robotics. IEEE. 2017 IEEE conference on cognitive and computational aspects of situation management (CogSIMA); 1-5.

Clark, J., & Jeremy, J. (1996). Attacking authentication protocols. High Integr. Syst., 1: 465-474.

Clearswift. (2019). Clearswift Security Research. (August). Retrieved from https://www.vansonbourne.com/client-research/10061901lh%0D

Coldewey, D. (2015). Hello Barbie, Goodbye Privacy? Expert Says Connected Doll Has Security Issues. NBC news. (December, 4). Retrieved from https://www.nbcnews.com/tech/gadgets/hello-barbie-goodbye-privacy-expert-says-connected-doll-has-security-n474446

Coley, R. L., & Hoffman, L. W. (1996). Relations of parental supervision and monitoring to children's functioning in various contexts: Moderating effects of families and neighborhoods. Journal of Applied Developmental Psychology, 17(1): 51-68.

CommunicationsAllianceLtd. (2019). "G660:2018 Assisting Customers Experiencing Domestic and Family Violence Industry Guideline," Communications Alliance Ltd, Sydney, Oct. 2018. Accessed: Jun. 23, 2019. [Online]. Available: https://commsalliance.com.au/__data/assets/pdf_file/0003/61527/Comm.

Crawford, D., & Sherman, J. (2018). Gaps in United States federal government IoT security and privacy policies. Journal of Cyber Policy 3(2): 187-200.

Crouter, A. C., & Head, M. R. (2002). Parental monitoring and knowledge of children. Handbook of parenting, 3, 461-483.

Crowell, C. R., Segerson, J., Kajzer, M. D., Villano, M., Zenk, J., Wegner, V., & Bell, M. M. (2020). Using Luring Communication Theory to Analyze the Behavior of Online Sexual Offenders. In Encyclopedia of Criminal Activities and the Deep Web (pp. 547-564). IGI Global.

Cyberdefense. (2019). Ransomware and the Internet of Things. (September, 21). Retrieved from https://www.cyberdefensemagazine.com/ransomware-and-the-internet-of-things/

Cyr, B., Horn, W., Miao, D., & Specter, M. (2014). Security analysis of wearable fitness devices (fitbit). Massachusetts Institute of Technology 1.

Das, D., Maity, S., Chatterjee, B., & Al., E. (2019). Enabling Covert Body Area Network using Electro-Quasistatic Human Body Communication. Science 9: 4160.

Davis, J. (2018a). AI, IoT, Medical Devices Top Health Cybersecurity Predictions for 2019. (December, 13). Retrieved from https://healthitsecurity.com/news/ai-iot-medical-devices-top-health-cybersecurity-predictions-for-2019

Davis, J. (2018b). When medical devices get hacked, hospitals often don't know it. Healthcare IT News. (May, 11). Retrieved from https://www.healthcareitnews.com/news/when-medical-devices-get-hacked-hospitals-often-dont-know-it

Davis, J. (2019). 82% IoT Devices of Health Providers, Vendors Targeted by Cyberattacks. Health It Security. https://healthitsecurity.com/news/82-iot-devices-of-health-providers-vendors-targeted-by-cyberattacks.

Dehmer, G. J., Jennings, J., Madden, R. A., Malenka, D. J., Masoudi, F. A., McKay, C. R., ..., ... Rumsfeld, J. S. (2016). The National cardiovascular data registry voluntary public reporting program: an interim report from the NCDR public reporting Advisory group. Journal of the American College of Cardiology 67(2): 205-215.

Doffman, Z. (2019). FDA Warns Of Dangerous Cybersecurity Hacking Risk With Connected Medical Devices. (June, 28). Forbes. Retrieved from https://www.forbes.com/sites/zakdoffman/2019/06/28/fda-issues-cybersecurity-warning-over-hacking-risk-for-connected-medical-devices/

Doukas, C., & Maglogiannis, I. (. (2012). Bringing IoT and cloud computing towards pervasive healthcare. IEEE. 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing: 922-926.

Downey, A. (2020). Encryption standards for medical devices 'need to be mandatory'. Digitalhealth.com., (October). Retrieved from https://www.digitalhealth.net/2019/07/encryption-standards-medical-devices-mandatory/

Doyle, T., & Veranas, J. (2014). Public anonymity and the connected world. Ethics and information technology, 16(3), 207-218.

Dragiewicz, M., & et al. (2018). "Technology facilitated coercive control: domestic violence and the competing roles of digital

media platforms," Feminist Media Studies, vol. 18, no. 4, pp. 609–625.

Duerager, A., & Livingstone, S. (2012). How can parents support children's internet safety? EUKids Online. http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20III/Reports/ParentalMediation.pdf.

EPIC-FTC. (2016). Complaint and Request for Investigation, Injunction, and Other Relief. Submitted by The Electronic Privacy Information Center, The Campaign for a Commercial Free Childhood, The Center for Digital Democracy, and Consumers Union. https://epic.org/privacy/ki.

EUaC. (2020). Standardisation and the EU Cybersecurity Act. EU Agency for Cybersecurity (previously the European Network and Information Systems Agency (ENISA)., (February 4). Retrieved from https://www.enisa.europa.eu/news/enisa-news/standardisation-and-the-eu-cybersecurity-act-1

FBI. (2017). Consumer Notice: Internet-Connected Toys Could Present Privacy And Contact Concerns For Children. Federal Bureau of Investigation. Public Service Announcement. https://www.ic3.gov/media/2017/170717.aspx.

Fitbit. (2018). Fitbit Community Grows to More Than 25 Million Active Users in 2017. Press Release.(1/8/2018). Retrieved from https://investor.fitbit.com/press/press-releases/press-release-details/2018/Fitbit-Community-Grows-to-More-Than-25-Million-Active-Users-in-2017/default.aspx

Foucault, M. (1977). Panopticism. Discipline and Punish: The Birth of the Prison, 195–317.

Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T., & N. Dell. (2018). "'A Stalker's Paradise': How Intimate Partner Abusers Exploit Technology," in Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, New York, NY, USA, p. 667:1–667:13,.

Gámez-Guadix, M., & Mateos-Pérez, E. (2019). Longitudinal and reciprocal relationships between sexting, online sexual solicitations, and cyberbullying among minors. Computers in Human Behavior, 94: 70-76.

Ghosh, A. K., Badillo-Urquiola, K., Guha, S., LaViola Jr, J. J., & Wisniewski, P. J. (2018). Safety vs. surveillance: what children have to say about mobile apps for parental control. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (pp. 1-14).

Gillespie, A. (2010). Legal definitions of child pornography. Journal of Sexual Aggression, 16: 19-31.

Gottlieb, S. (2018). Statement from FDA Commissioner Scott Gottlieb, M.D. on FDA's efforts to strengthen the agency's medical device cybersecurity program as part of its mission to protect patients. US FDA. https://www.fda.gov/news-events/press-announcements/statement-fda-com.

Hardesty, L. (2013). How Hard Is It to "De-Anonymize" Cellphone Data? MIT News Office. https://news.mit.edu/2013/how-hard-it-de-anonymize-cellphone-data.

Harkin, D., Molnar, A., & E. Vowles. (2020). "The commodification of mobile phone surveillance: An analysis of the consumer spyware industry," Crime, Media, Culture, vol. 16, no. 1, pp. 33–60.

Harris, B. A., & D. Woodlock. (2018). "Digital Coercive Control: Insights from Two Landmark Domestic Violence Studies," Br J Criminol.

Havron, S., Freed, D., Chatterjee, R., McCoy, D., Dell, N., & T. Ristenpart. (2019). "Clinical computer security for victims of intimate partner violence," in 28th USENIX Security Symposium, Santa Clara, CA, 2019, pp. 105–122.

Henry, N., & A. L. G. Flynn. (2020). "Technology-Facilitated Abuse among Culturally and Linguistically Diverse Woman: A Qualitative Study," Office of the eSafety Commissioner, Canberra, 2018. Accessed: May 26, 2020. [Online]. Available: https://research.monash.edu/en/publications/technology-.

Hern, A. (2017). CloudPets stuffed toys leak details of half a million users. The Guardian. (February, 28). Retrieved from https://www.theguardian.com/technology/2017/feb/28/cloudpets-data-breach-leaks-details-of-500000-children-and-adults

Hockey, A. (2020). Uncovering the cyber security challenges in healthcare. Network Security 2020(4); 18-19.

Holloway, D., & Green, L. (2016). The Internet of toys. Communication Research and Practice, 00(00), 1–14. https://doi.org/10.1080/22041451.2016.1266124

Hunt, T. (2017). Data from connected CloudPets teddy bears leaked and ransomed, exposing kids' voice messages. Troyhunt.com. (February, 28). Retrieved from https://www.troyhunt.com/data-from-connected-cloudpets-teddy-bears-leaked-and-ransomed-exposing-kids-voice-messages/

IHE. (2015). Medical Device Software Patching. Integrating the Healthcare Enterprise, Patient Care Device Domain (IHE PCD) in Cooperation with the Medical Device Innovation, Safety and Security (MDISS) Consortium White Paper. https://ihe.net/uploadedFiles/Documents/PC.

IoTBusiness. (2019). Lack of Cybersecurity Investments in Smart Cities Will Seed the Future IoT Vulnerabilities. (August, 20). Retrieved from https://iotbusinessnews.com/2019/08/20/50003-lack-of-cybersecurity-investments-in-smart-cities-will-seed-the-future-iot-vulnerabilities/

IoTBusiness. (2020). Why We Need to Start Incorporating Better Cybersecurity Measures for IoT Devices Used by Health Organizations. (October, 6). Retrieved from https://iotbusinessnews. com/2020/10/06/99940-why-we-need-to-start-incorporating-better-cybersecurity-measures-for-iot-devices-used-by-health-organizations/

Irdeto. (2019). Patient Safety at Risk from Unsecured Healthcare IoT Says Irdeto Research. https://wp-dev.irdeto.com/news/patient-safety-at-risk-from-unsecured-healthcare-iot-says-irdeto-research/.

ISO. (2006). ISO/IEC 62304:2006 Medical device software — Software life cycle processes. International Standards Organisation. https://www.iso.org/standard/38421.html.

J. Slupska. (2019). "Safe at Home: Towards a Feminist Critique of Cybersecurity," St Antony's International Review, vol. 15, no. 1, pp. 83–100.

Jackson Jr, G. W., & Rahman, S. (2019). Exploring Challenges and Opportunities in Cybersecurity Risk and Threat Communications Related To The Medical Internet Of Things (MIoT). arXiv preprint arXiv:1908.00666.

Janes, B., Crawford, H., & T. OConnor. (2020). "Never Ending Story: Authentication and Access Control Design Flaws in Shared IoT Devices," in IEEE Security and Privacy SafeThings Workshop, San Francisco, May 2020, p. 6, [Online]. Available: https://cdn.technadu.com/wp-content/uploads/2020/06/research_.

Jones, M. L., & Meurer, K. (2016). Can (and Should) Hello Barbie Keep a Secret?. IEEE Ethics.

Jonsson, F., & Tornkvist, M. (2017). RSA authentication in Internet of Things: Technical limitations and industry expectations. KTH Roy. Inst. Technol., Stockholm, Sweden. https://www.diva-portal.org/smash/get/diva2:1112039/FULLTEXT01.pdf.

Juniper-Research. (2018). Smart Toy Revenues To Grow By Almost 200% From 2018 To $18 Billion By 2023. Juniper Research. (May 8). Retrieved from https://www.juniperresearch.com/press/press-releases/smart-toy-revenues-grow-almost-200pc-by-2023

Kelion, L. (2015). Google patents "creepy" internet toys to run the home. (May 22)., (May). Retrieved from https://www.bbc.co.uk/news/technology-32843518

Keller, M. H., & Dance, G. J. X. (2019). The Internet Is Overrun With Images of Child Sexual Abuse. What Went Wrong? The New York Times. https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html.

Khoo, C., Robertson, K., & R. J. Deibert. (2019). "Installing Fear: Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications," Citizen Lab, Toronto, 120.

Kirwil, L. (2009). Parental mediation of children's internet use in different European countries. Journal of Children and Media, 3(4): 394–409.

Kloess, J. A., Beech, A. R., & Harkins, L. (2014). Online child sexual exploitation: Prevalence, process, and offender characteristics. Trauma, Violence, & Abuse, 15(2): 126-139.

Kramer, R. M. (1999). Trust and distrust in organizations: Emerging perspectives, enduring questions. Annual Review of Psychology, 50(1), 569–598.

L. M. Tanczer. (2019). "The Government published its draft domestic abuse bill, but risks ignoring the growing threat of tech abuse," Medium, Feb. 25, 2019. https://medium.com/policy-postings/the-government-published-its-draft-domestic-abuse-bill-but-risks-ignoring-the-growing-.

Laughlin, A. (2017). Safety alert: see how easy it is for almost anyone to hack your child's connected toys. Which?. (November, 14). Retrieved from https://www.which.co.uk/news/2017/11/safety-alert-see-how-easy-it-is-for-almost-anyone-to-hack-your-childs-connected-toys/

Lee, G. (2019). What roles should the government play in fostering the advancement of the internet of things?. Telecommunications Policy, 43(5): 434-444.

Littman, S. D. (2011). Point/counterpoint: proactive parenting privacy and youth. American Library Association. http://youthprivacy.ala.org/2011/05/05/pointcounterpoint-sarah-darerlittman-on-proactive-parenting.

Livingstone, S. (2008). Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. New media & society, 10(3), 393-411.

Livingstone, S., & Bober, M. (2006). Regulating the Internet at home: Contrasting the perspectives of children and parents. In D. Buckingham & R. Willett (Eds.), Digital generations: Children, young people, and new media (pp. 93–113). Mahwah, NJ: Lawrence Erlbaum Associates, Publishers.

Lloyds. (2018). Networked world Risks and opportunities in the Internet of Things. Lloyds of London. Emerging Risk Report 2018 Technology. Retrieved from https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/networked-world ?utm_source=UCL_website&utm_medium=referral&utm_campaign=emergingrisks_networkedworld

Lomas, N. (2017a). Call to ban sale of IoT toys with proven security flaws. Techcrunch. (November, 15). Retrieved from https://

techcrunch.com/2017/11/15/call-to-ban-sale-of-iot-toys-with-proven-security-flaws/

Lomas, N. (2017b). Consumer report warns over safety of kids' smartwatches. Techcrunch. (October, 19).

Lopez-Neira, I., Patel, T., Parkin, S., Danezis, G., & L. M. Tanczer. (2019). "'Internet of Things': How abuse is getting smarter," Safe – The Domestic Abuse Quarterly, no. 63, pp. 22–26.

Lord, N. (2020). Healthcare Cybersecurity: Tips for Securing Private Health Data. Retrieved from https://digitalguardian.com/blog/healthcare-cybersecurity-tips-securing-private-health-data

Maddox, T. (2015). The dark side of wearables: How they're secretly jeopardizing your security and privacy. (October, 7). Retrieved from https://www.techrepublic.com/article/the-dark-side-of-wearables-how-theyre-secretly-jeopardizing-your-security-and-privacy/

Malan, D., Fulford-Jones, T., Welsh, M., & Moulton, S. (2004). Codeblue: an ad hoc sensor network infrastructure for emergency medical care. Proceedings of the International Workshop on Wearable and Implantable Body Sensor Networks 5 (April).

Markwick, K., Bickerdike, A., Wilson-Evered, E., & Zeleznikow, J. (2019). "Technology and Family Violence in the Context of Post-Separated Parenting," Australian and New Zealand Journal of Family Therapy, vol. 40, no. 1, pp. 143–162, 2019, doi: 10.1002/anzf.1350.

Mathiesen, K. (2013). The Internet, children, and privacy: the case against parental monitoring. Ethics and Information Technology, 15(4), 263-274.

Matthews, T., & et al. (2017a). "Security and Privacy Experiences and Practices of Survivors of Intimate Partner Abuse," IEEE Security Privacy, vol. 15, no. 5, pp. 76–81.

Matthews, T., & et al. (2017b). "Stories from Survivors: Privacy & Security Practices when Coping with Intimate Partner Abuse," in Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, New York, NY, USA.

Mayhew, J., & H. Jahankhani. (2020). "Combating Domestic Abuse inflicted in Smart Societies," in Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity, H. Jahankhani, S. Kendzierskyj, N. Chelvachandran, and J. Ibarra, Eds. Cham: Springer International Publishing.

Messing, J., Bagwell-Gray, M., Brown, M. L., Kappas, A., & Durfee, A. (2020). Intersections of Stalking and Technology-Based Abuse: Emerging Definitions, Conceptualization, and Measurement. Journal of Family Violence. https://doi.org/10.1007/s10896-019-00114-7

McGlynn, C., Rackley, E., & Johnson, K. (2019).

"Shattering lives and myths: A report on image-based sexual abuse.," Durham, Kent:, Durham University; University of Kent, Project Report. doi: 10/shattering-lives-and-myths-revised-aug-2019.pdf.

Mckinlay, T., & T. Lavis. (2020). "Why did she send it in the first place? Victim blame in the context of 'revenge porn,'" Psychiatry, Psychology and Law, vol. 0, no. 0, pp. 1–11.

MDCG. (n.d.). MDCG 2019-16 Guidance on Cybersecurity for medical devices July 2020 rev.1. Medical Devices Coordination Group. https://cemarking.net/medical-device-regulation-mdr-new-guidance-documents-published/.

Medtronic. (2020). Carelink 2090 And Carelink Encore 29901 Programmers security Bulletin. (First published February, 2018; updated October 2018; January 2020). Retrieved from https://global.medtronic.com/xg-en/product-security/security-bulletins/carelink-2090-29901.html

Medvedeva, A. S., & Dozortseva, E. G. (2019). Features of online grooming as a form of sexual exploitation of minors (based on the analysis of communication between adults and children in the Internet). Psychology and Law, 9(4): 161-173.

Memon, M. H., Memon, M. H., Marium, S. M., & Khan, J. (2020). Security and Privacy Issues of Medical Systems in Wireless Sensor Networks: A Survey. Asian Journal For Convergence In Technology (AJCT) 5(3): 08-12.

Merdian, H. L., Perkins, D. E., Webster, S. D., & McCashin, D. (2019). Transnational child sexual abuse: outcomes from a roundtable discussion. International journal of environmental research and public health, 16(2), 243.

Messing, J., Bagwell-Gray, M., Brown, M. L., Kappas, A., & A. Durfee. (2020). "Intersections of Stalking and Technology-Based Abuse: Emerging Definitions, Conceptualisation, and Measurement," J Fam Viol.

MHRA. (2014). Guidance on legislation Borderlines with medical devices. UK Medicines and Healthcare Products Regulatory Agency. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/284505/Borderlines_with_medical_devices.pdf.

Mills, E. (2011). Researcher battles insulin pump maker over security flaw. CNET. (August, 26). Retrieved from https://www.cnet.com/news/researcher-battles-insulin-pump-maker-over-security-flaw/

Moganedi, S. (2018). Undetectable Data Breach in IoT: Healthcare Data at Risk. 17th European Conference on Cyber Warfare and Security 2: 296.

Morley, N. (2016). Paedophiles are hiding child

abuse images on fake porn websites. (April, 21). Retrieved from https://metro.co.uk/2016/04/21/paedophiles-are-hiding-child-abuse-images-on-fake-porn-websites-5832489/

N. Bowles. (2018). "Thermostats, Locks and Lights: Digital Tools of Domestic Abuse," The New York Times, New York.

NHSDigital. (2020). Changes to how we assess apps and tools. Retrieved from https://digital.nhs.uk/services/nhs-apps-library#how-the-assessment-works

Nikander, P., Siegel, J. E., & Viitala, R. (2020). Mustapää, T., Autiosalo, J., Digital Metrology for the Internet of Things. In 2020 Global Internet of Things Summit (GIoTS) (pp. 1-6). IEEE.

Nikolovska, M. (2020). The Internet as a creator of a criminal mind and child vulnerabilities in the cyber grooming of children. JYU dissertations.

Nissenbaum, H. (2001). How computer systems embody values. Computer (34)3: 120-119.

Nissenbaum, H. (2004). Privacy as contextual integrity. Wash. L. Rev., 79, 119.

Norwegian-Consumer-Council. (2017). #WatchOut. Analysis of smartwatches for children. Report. https://fil.forbrukerradet.no/wpcontent/uploads/2017/10/watchout-rapport-october-2017.pdf.

Novinson, M. (2020). The 10 Biggest Data Breaches of 2020 (So Far). (June, 26). Retrieved from https://www.crn.com/slide-shows/security/the-10-biggest-data-breaches-of-2020-so-far-

Nuttall, L., Evans, J., Franklin, M., & S. Burne James. (2020). "Coercive Control Resistant Design: The Key To Safer Technology," IBM Corporation, London, 2019. Accessed: Aug. 08, 2020. [Online]. Available: https://www.ibm.com/blogs/policy/wp-content/uploads/2020/05/CoerciveControlResistantDesign.pdf.

Oberhaus, D. (2020). The future of health care is wearable. (March, 30). Retrieved from https://asunow.asu.edu/20200323-solutions-future-health-care-wearable

ONS. (2019). Office for National Statistics, "Domestic abuse prevalence and trends, England and Wales: year ending March 2019," Nov. 25, 2019. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/revalenceandtrendsenglandandwales/.

P. L. Sweet. (2019). "The Sociology of Gaslighting," Am Sociol Rev, vol. 84, no. 5, pp. 851–875.

Parkin, S., Patel, T., Lopez-Neira, I., & L. M. Tanczer. (2019). "Usability analysis of shared device ecosystem security: informing support for survivors of IoT-facilitated tech-abuse," in Proceedings of the New Security Paradigms Workshop, San Carlos, Costa Rica.

Peppet, S. (2016). Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent. Texas Law Review, 93: 85-176.

Picchi, A. (2016). Your kids' toys could be spying on your family. CBS News. Retrieved from https://www.cbsnews.com/news/your-kids-toys-could-be-spying-on-your-family/

Pinto, L., & Nemorin, S. (2014). Who's the Boss? "The Elf on the Shelf" and the normalization of surveillance. Canadian Centre for Policy Alternatives. https://www.policyalternatives.ca/publications/commentary/whos-boss.

Ponemon-Institute. (2017). Medical Device Security: An Industry Under Attack and Unprepared to Defend. Ponemon Institute LLC. Research Report Sponsored by Synopsys. file:///Users/SDatta/Downloads/medical-device-security-ponemon-synopsys.pdf.

Powell, A., & N. Henry. (2018). "Policing technology-facilitated sexual violence against adult victims: police and service sector perspectives," Policing and Society, vol. 28, no. 3, pp. 291–307.

PsycholoGenie. (n.d.). 6 Types of Child Abuse that Everyone Should Know About. Retrieved from https://psychologenie.com/types-child-abuse

R. Leitão. (2019). "Anticipating Smart Home Security and Privacy Threats with Survivors of Intimate Partner Abuse," in Proceedings of the 2019 on Designing Interactive Systems Conference, San Diego, CA, USA.

R. Scammell. (2019). PCM Data Breach Highlights Risks of Third-Party Cloud Providers. https://www.verdict.co.uk/pcmdata-breach-cloud-providers/.

Radcliff, J. (2019). PEAC Presentation: Patient turned Hacker. FDA.gov. (July, 13). Retrieved from https://www.fda.gov/media/130719/download

RAENG. (2018). Cyber safety and resilience. Royal Academy of Engineering. Retrieved from https://www.raeng.org.uk/publications/reports/cyber-safety-and-resilience

Rahman, M., Carbunar, B., & Banik, M. (2013). Fit and vulnerable: Attacks and defenses for a health monitoring device. arXiv preprint arXiv:1304.5672.

Rawlinson, K. (2015). HP study reveals smartwatches vulnerable to attack. HP News.

Refuge. (2020). "72% of Refuge service users identify experiencing tech abuse," Refuge Charity - Domestic Violence Help, Jan. 09, 2020. https://www.refuge.org.uk/72-of-refuge-service-users-identify-experiencing-tech-abuse/ (accessed Mar. 01, 2020).

Rodríguez-Rodríguez, I., Rodríguez, J.-V., Elizondo-Moreno, A., Heras-González, P., & M. Gentili. (2020). I. Rodríguez-Rodríguez, J.-V. Rodríguez, A. Elizondo-Moreno, P.

Heras-González, and M. Gentili, "Towards a Holistic ICT Platform for Protecting Intimate Partner Violence Survivors Based on the IoT Paradigm," Symmetry, vol. (1), Art. no. 1.

Rosenblum, A. (2015). Your Doctor Doesn't Want to Hear About Your Fitness-Tracker Data. November 24. MIT Technology Review.

Rotenberg, K. J. (2010). The conceptualization of interpersonal trust: A basis, domain, and target framework. In K. J. Rotenberg (Ed.), Interpersonal trust during childhood and adolescence (pp. 8–27). New York: Cambridge University Press.

Russell, A., Pettit, G. S., & Mize, J. (1998). Horizontal qualities in parent-child relationships: Parallels with and possible consequences for children's peer relationships. Developmental Review, 18(3), 313–352.

Safavi, S., & Shukur, Z. (2014). Improving google glass security and privacy by changing the physical and software structure. Life Science Journal 11(5): 109-117.

Samani, R., Honan, B., & Reavis, J. (2015). Chapter 8–Cloud Security Alliance Research. CSA guide to cloud computing, syngress, 149-169.

Sambasivan, N., & et al. (2019a). "'Privacy is not for me, it's for those rich women': Performative Privacy Practices on Mobile Phones by Women in South Asia," in Proceedings of the Fourteenth Symposium on Usable Privacy and Security, Baltimore, MD, USA, 2018, pp. 127–142, Accessed: Jul. .

Sambasivan, N., & et al. (2019b). "'They Don'T Leave Us Alone Anywhere We Go': Gender and Digital Abuse in South Asia," in Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, New York, NY, USA.

Sambasivan, N., & et al. (2019c). "Toward Gender-Equitable Privacy and Security in South Asia," IEEE Security Privacy, vol. 17, no. 4, pp. 71–77.

Schwartz, J. (2016). Show Me the Money: Financial Sector A Big Target for Cyberattacks. (July, 5). Retrieved from https://www.mediapro.com/blog/financial-sector-target-cyberattacks/

Scott, R., Borchert, O., Mitchell, S., & Connelly, S. (2020). NIST Special Publication 800-207: Zero Trust Architecture. National Institute of Standards and Technology. US Department of Commerce. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

Seagren, E. (2011). Chapter 8 - Security as an Ongoing Process. In Secure your network for free. Elsevier. Pages 447-473.

Seals, T. (2018). CloudPets May Be Out of Business, But Security Concerns Remain. Threat Post. (June, 7). Retrieved from https://threatpost.com/cloudpets-may-be-out-of-business-but-security-concerns-remain/132609/

Shinder, T. W., Diogenes, Y., & Shinder, D. L. (2013). Chapter 5—Patch Management with Windows Server. In Windows server 2012 security from end to edge and beyond: Architecting, designing, planning, and deploying windows server 2012 security solutions. Newnes.

Slupska, J., & L. M. Tanczer. (n.d.). "Intimate Partner Violence (IPV) Threat Modeling: Tech abuse as cybersecurity challenge in the Internet of Things (IoT)," in Handbook on Technology-Facilitated Violence and Abuse: International Perspectives and Experiences, J. Bailey, A. Flynn, and N. Hen.

Smetna, J. G. (2010). The role of trust in adolescent–parent relationships: To trust is to tell you. In K. J. Rotenberg (Ed.), Interpersonal trust during childhood and adolescence (pp. 223–246). New York: Cambridge University Press.

Smith, J. M. (2020). "Intimate Partner Femicide: Using Foucauldian Analysis to Track an Eight Stage Progression to Homicide," Violence Against Women, vol. 26, no. 11, pp. 1267–1285.

Sposito, S. (2015). How Mattel's Hello Barbie could become a target for hackers. (October, 12). The Sydney Morning Herald. Retrieved from https://www.smh.com.au/technology/how-mattels-hello-barbie-could-become-a-target-for-hackers-20151011-gk6ahv.html

Stadt-Wien. (2020). Frauenstadträtin Kathrin Gaal: Cybergewalt: Start für neue Kompetenzstelle der Stadt Wien. City of Vienna: Vienna.

Stanley, J. (2001). Child abuse and the Internet. Australian Institute Of Family Studies. National Child Protection Clearinghouse Issue 15 (June). https://aifs.gov.au/cfca/sites/default/files/publication-documents/issues15.pdf.

Storm, D. (2015). Google's Internet-connected toys patent sparks privacy concerns , visions of IoT Chucky. Computerworld, (May 25). Retrieved from https://www.computerworld.com/article/2926333/googles-internet-connected-toys-patent-sparks-privacy-concerns-visions-of-iot-chucky.html

Sun, Z., Schuster, R., & Shmatikov, V. (2020). De-Anonymizing Text by Fingerprinting Language Generation. arXiv preprint arXiv:2006.09615.

Swinhoe, D. (2020). The 15 biggest data breaches of the 21st century. (April, 17). Retrieved from https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

Tanczer, L., Carr, M., Brass, I., Steenmans, I., & Blackstock, J. (2017). IoT and Its Implications for Informed Consent (July 25,

2017). PETRAS IoT Hub, STEaPP: London. Available at SSRN: https://ssrn.com/abstract=3117293 or http://dx.doi.org/10.2139/ssrn.3117293.

Tanczer, L. M. (2013). "Post, Gender, Internet?," C. Landler, P. Parccek, and M. C. Kettemann, Eds. Krems: Internet & Gesellschaft Collaboratory AT, 2013, pp. 53–69.

Tanczer, L. M., Lopez-Neira, I., Parkin, S., Patel, T., & G. Danezis. (2018). "Gender and IoT (G-IoT) Research Report: The rise of the Internet of Things and implications for technology-facilitated abuse," University College London, London, Nov. 2018. [Online]. Available: https://www.ucl.ac.uk/steapp/sites/steapp/files/giot-report.

Tanczer, L. M., Patel, T., Parkin, S., & G. Danezis. (2018). "Gender and IoT (G-IoT) Tech Abuse Guide: How internet-connected devices can affect victims of gender-based domestic and sexual violence and abuse," University College London, London, May 2018. Accessed: Jun. 18, 2018. [Online]. Available: https://www.ucl.

Tanczer, L. M., Patel, T., Parkin, S., Lopez-Neira, I., & J. Slupska. (2018). "Written Submission to the Online Harms White Paper Consultation," University College London, London, Jun. 2019. Accessed: Jun. 18, 2018. [Online]. Available: https://www.ucl.ac.uk/steapp/sites/steapp/files/online_harms_white_paper_consultation_response_g.

Tanczer, Leonie Maria, Brass, I., Elsden, M., Carr, M., & Blackstock, J. (2019). The United Kingdom's Emerging Internet of Things (IoT) Policy Landscape. In R. Ellis & V. Mohan (Eds.), Rewired: Cybersecurity Governance (pp. 37–56). Hoboken, New Jersey: Wiley.

Tech UK. (2019). "The state of the connected home," Tech UK, London, 3, Jun. 2019. [Online]. Available: http://www.techuk.org/images/assets/Connected_Home/The_State_of_the_Connected_Home_Edition3_Jun19.pdf.

TheGuardian. (2015). UK child protection officers receive one sexting-related case every day. The Guardian. (June, 15). Retrieved from https://www.theguardian.com/uk-news/2015/jun/15/uk-child-protection-officers-one-sexting-related-case-every-day

Tolentino, M. (n.d.). Security Challenges for Fitbit, Google Glass+ Other Wearable Devices.

Tseng, E., & et al. (2020). "The Tools and Tactics Used in Intimate Partner Surveillance: An Analysis of Online Infidelity Forums," in 29th Security Symposium (USENIX) Security 20, Online, Aug. 2020, pp. 1893–1909, Accessed: Aug. 08, 2020. [Online]. Available: https://www.usenix.org.

Turner, S. (2020). Connected Toys: What Device Documentation Explains about Privacy and Security. https://doi.org/10.14324/000.rp.10100395

Turner, S., Quintero, J. G., Turner, S., Lis, J., & Tanczer, M. (2020). The exercisability of the right to data portability in the emerging Internet of Things (IoT) environment, (X). https://doi.org/10.1177/1461444820934033

Tynan, D. (2017). How Hospitals Use Network Microsegmentation to Guard Against Cyberattacks. (October, 25). Retrieved from https://healthtechmagazine.net/article/2017/10/how-hospitals-use-network-microsegmentation-guard-against-cyberattacks

UCLSTEaPP. (2018). "UCL runs a digital security training event aimed at domestic abuse support services," UCL Department of Science, Technology, Engineering and Public Policy, Nov. 19, 2018. https://www.ucl.ac.uk/steapp/news/2018/nov/ucl-runs-digital-security-training-event.

UK-CoP. (2018). Code of Practice for Consumer IoT Security. UK Department of Digital, Culture, Media and Sport.

UNICEF. (2019). Memorandum on Artificial Intelligence and Child Rights. UNICEF Innovation. Human Rights Center, UC Berkeley. https://www.unicef.org/innovation/reports/memoAIchildrights.

University-of-Massachusetts-Amherst. (2008). How Much Security Do You Expect From Your Pacemaker? UMass Amherst Expert Works to Provide Cyber Trust. University of Massachusetts Amherst. Retrieved from https://www.umass.edu/newsoffice/article/how-much-security-do-you-expect-your-pacemaker-umass-amherst-expert-works-provide-cyber

UNODC. (2018). United Nations Office on Drugs and Crime, "Global Study on Homicide 2018: Gender-related killing of women and girls," United Nations, Vienna, 2018. Accessed: Aug. 09, 2020. [Online]. Available: https://www.unodc.org/documents/data-and-analysis/GSH2018/GSH.

US-DHS. (2020). ICS Medical Advisory (ICSMA-19-080-01) Medtronic Conexus Radio Frequency Telemetry Protocol (Update B). Cybersecurity & Infrastructure Security Agency. United States Department of Homeland Security. (June, 4). Retrieved from https://us-cert.cisa.gov/ics/advisories/ICSMA-19-080-01

USFDA. (n.d.). The FDA's Role In Medical Device Cybersecurity FDA Fact Sheet. Dispelling Myths and Understanding Facts. U.S. Food and Drug Administration. https://www.fda.gov/media/123052/download.

USFDA. (2019a). 2019 Medical Device Recalls. (December, 20). Retrieved from https://www.fda.gov/medical-devices/medical-device-recalls/2019-medical-device-recalls

USFDA. (2019b). Device Software Functions Including Mobile Medical Applications. USFDA. https://www.fda.gov/medical-

devices/digital-health/device-software-functions-including-mobile-medical-applications.

USFDA. (2019c). General Wellness: Policy for Low Risk Devices. Guidance for Industry and Food and Drug Administration Staff. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/general-wellness-policy-low-risk-devices.

USFDA. (2020). SweynTooth Cybersecurity Vulnerabilities May Affect Certain Medical Devices: FDA Safety Communication. US FDA. (March, 3). Retrieved from https://www.fda.gov/medical-devices/safety-communications/sweyntooth-cybersecurity-vulnerabilities-may-affect-certain-medical-devices-fda-safety-communication

Valente, J., & Cardenas, A. A. (2017). Security & privacy in smart toys. In Proceedings of the 2017 Workshop on Internet of Things Security and Privacy: 19-24.

Verizon. (2020). "2020 Data Breach Investigations Report". Verizon. https://enterprise.verizon.com/resources/reports/dbir/.

Vitis, L., & Gilmour, F. (2017). "Dick pics on blast: A woman's resistance to online sexual harassment using humour, art and Instagram," Crime, Media, Culture, vol. 13, no. 3, pp. 335–355.

VPNMentor. (2020). Security and Privacy Flaws Discovered on Popular Wearable Devices. Retrieved from https://www.vpnmentor.com/blog/security-and-privacy-flaws-discovered-on-popular-wearable-devices/

Walker, K., & Sleath, E. (2017). "A systematic review of the current knowledge regarding revenge pornography and non-consensual sharing of sexually explicit media," Aggression and Violent Behavior, vol. 36, no. September-October, pp. 9–24.

Wallace, L. N. (2020). Web-Based Child Sexual Exploitation. In Encyclopedia of Criminal Activities and the Deep Web (pp. 533-546). IGI Global.

Walsh, M. (2017). My Friend Cayla doll banned in Germany over surveillance concerns. ABCNews. Retrieved from https://www.abc.net.au/news/2017-02-18/my-friend-cayla-doll-banned-germany-over-surveillance-concerns/8282508

Weisskopf, M. (2007). Who Regulates America's Toymakers? TIME. (August, 18). Retrieved from http://content.time.com/time/business/article/0,8599,1654132,00.html

Williams, J. G. (2014). Change Management: Security and Patch Information Knowledge. In Introduction to Information Security, 201-231.

Winkler, V. J. (2011). Securing the Cloud: Cloud computer Security techniques and tactics. Elsevier.

WomensAid. (2020). "Women's Aid responds to the Budget," Womens Aid, Mar. 11, 2020. https://www.womensaid.org.uk/womens-aid-responds-to-the-budget/ (accessed Aug. 10, 2020).

Woodlock, D. (2014). "Technology-facilitated stalking: Findings and resources from the SmartSafe project," Domestic Violence Resource Centre Victoria, Collingwood.

Woodlock, D. (2017). "The Abuse of Technology in Domestic Violence and Stalking," Violence Against Women, vol. 23, no. 5, pp. 584–602.

Yaacoub, J. P. A., Noura, M., Noura, H. N., Salman, O., Yaacoub, E., Couturier, R., & Chehab, A. (2020). Securing internet of medical things systems: limitations, issues and recommendations. Future Generation Computer Systems 105: 581-606.

Zahra, S. R., & Chishti, M. A. (2019). Ransomware and Internet of Things: A new security Nightmare. IEEE. 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence): 551-555.

Zhang, C., Jiang, H., Wang, Y., Hu, Q., Yu, J., & Cheng, X. (2019). User identity De-anonymization based on attributes. In International Conference on Wireless Algorithms, Systems, and Applications (pp. 458-469). Springer, Cham.
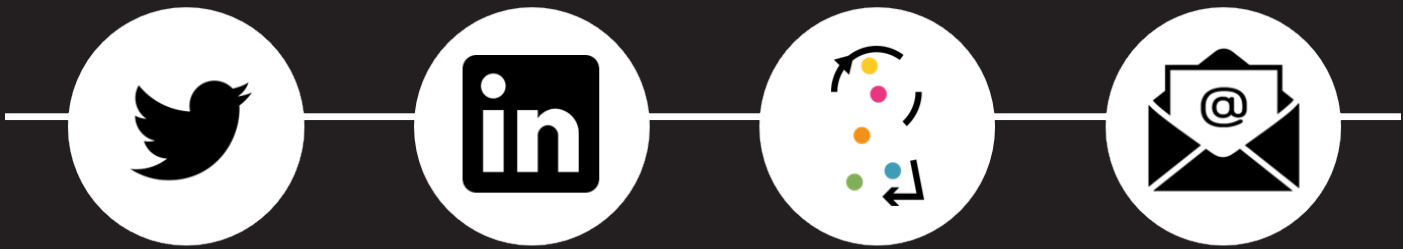
TWITTER
@PETRASiot

LINKEDIN
linkedin.
com/school/
petrasiot

WEBSITE
petras-iot.org

EMAIL
petras@ucl.
ac.uk