REPHRAIN

Protecting citizens online

Call for Evidence: Connected tech: smart or sinister?

This is a submission from the REPHRAIN centre. Specifically, the following researchers contributed to the formulation of this response (in alphabetical order): Dr Chuadhry Mujeeb Ahmed, Prof Madeline Carr, Dr Partha Das Chowdhury, Prof Lynn Coventry, Dr François Dupressoir, Dr David Ellis, Dr Nadin Kokciyan, Prof Shane D Johnson, Dr Jose Tomas Llanos, Dr Mark McGill, Dr Ola Michalec, Dr Inah Omoronyia, Dr Marvin Ramokapane, Prof Awais Rashid, Yvonne Rigby, Dr Bianca Slocombe, Dr Kami Vaniea, Dr Baraa Zieni.

UK Research and Innovation · University of Bristol · UCL · The University of Edinburgh · King's College London · University of Bath

June 2022

Call for Evidence: Connected tech: smart or sinister?

INTRODUCTION

Thank you for an opportunity to provide our response to this evidence call. We are writing on behalf of REPHRAIN, the National **Re**search Centre on **P**rivacy, **H**arm **R**eduction and **A**dversarial **I**nfluence O**n**line. REPHRAIN is the UK's world-leading interdisciplinary community focused on the protection of citizens online. As a UKRI-funded National Research Centre, we boast a critical mass of over 100 internationally leading experts at 13 UK institutions working across 37 different and diverse research projects and 23 founding industry, non-profit, government, law, regulation, and international research centre partners. As an interdisciplinary and engaged research group, we work collaboratively on addressing the three following missions:

- Delivering privacy at scale while mitigating its misuse to inflict harms
- Minimising harms while maximising benefits from a sharing-driven digital economy
- Balancing individual agency vs. social good.

We are addressing this call because REPHRAIN researchers are international experts on smart and connected technologies across domains like agriculture, energy, consumer electronics, smart home, financial technologies, and many others. For years, we have been working to identify, evaluate and address risks to smart systems in the areas like privacy, security, usability, responsibility, among the others.

This is a submission from the REPHRAIN centre. Specifically, the following researchers contributed to the formulation of this response (in alphabetical order): Dr Chuadhry Mujeeb Ahmed Prof Madeline Carr, Dr Partha Das Chowdhury, Prof Lynn Coventry, Dr François Dupressoir, Dr David Ellis, Dr Nadin Kokciyan, Prof Shane D Johnson, Dr Jose Tomas Llanos, Dr Mark McGill, Dr Ola Michalec, Dr Inah Omoronyia, Dr Marvin Ramokapane, Prof Awais Rashid, Yvonne Rigby, Dr Bianca Slocombe, Dr Kami Vaniea, Dr Baraa Zieni.

1. **What has been or will be the most important impacts of increasingly prevalent smart and connected technology in our lives, including in the home, in the workplace and in our towns and cities, and are they necessarily better than current systems?**

We believe that smart and connected technologies have brought about positive and negative impacts on the society, both requiring attention in the ongoing policy and regulatory processes.

Starting from the positives, we can outline the following:

- Major impacts will continue to combine the benefits of data linkage alongside the development of new data sources. For example, data linkage has allowed for individual health data to be linked with education data to **better understand associations between a lack of engagement with health care and reduced school attendance, higher levels of school exclusion and lower educational attainment** (McQueenie et al., 2021).

- Digital trace data provides **new opportunities for measurement** that captures behavioural, situational, and environmental/contextual factors simultaneously. For instance, mobile and wearable devices that we carry with us for large swathes of the day provide a collection of sensors and logging routines. These can be utilised to predict a variety of outcomes, from social interaction, personality, mood, to general health (Davidson et al., 2022).
- In the energy domain, smart meters have improved **forecasting of energy demand** depending on the consumer demographics, weather, or time of the day. Improved forecasting allows energy companies to purchase energy in more optimal amounts and times, bringing efficiencies to both company operations and customers' bills. It also allows for a better understanding of weather-related risks, so that suppliers can create contingency for cold snaps in winters (e.g., through buying cold weather insurance). Smart meters are foundational for building the future smart and sustainable infrastructure since they allow balancing between energy consumption and generation (Michalec et al., 2022)
- In the health domain, smart devices improved the **management of both chronic and acute conditions** e.g., pulse oximeters for Covid-19 and glucose monitoring for diabetes.
- In agriculture, smart technologies are already used to **support farmers to generate improved farm yield and profit**. Furthermore, smart technologies have been deployed in manufacturing to **optimise supply chain and efficient production**.
- Finally, smart devices are now used in cities to **improve transport** (e.g., real time public transport schedules) **and monitor environment** (e.g., air or water quality).

However, smart and connected technologies are reconfiguring our society in the following ways:

- **They require a new perspective on physical safety**. Connected devices pose risks to physical safety beyond data protection. Due to the cyber-physical nature of connected technologies, both functionality errors and cyber security attacks can result in harm to human health (e.g., through electric shock from an electronic device, self-driving car accident, incorrect glucose reading in a diabetic smart watch etc.). Another challenge pertaining safety of IoT devices is that they can be used to engage in harmful behaviours, e.g., stalking, intimate partner violence or eliciting private information. Our current approaches to validating and testing safety do not sufficiently consider the interconnected nature of smart devices (Michalec et al., 2022).
- **They require formation of novel software maintenance practices that encourage durability of smart devices**. There are no accepted protocols on long term software patching for devices with longer life expectancy (e.g., cars, home appliances) (Anderson, 2018; Golomb, 1971). Without a push for durable maintenance, there is a risk that cyber security of devices will stand in tension to environmental sustainability and lead to more e-waste (Privacy International, 2021).
- **They require a renewed public debate about the acceptable security risks and mitigations.** An overwhelming consequence of the adoption of smart devices is a significant increase in attack surface due to the unprecedented volume and granularity of data connected to the Internet. This might either lead to multiple scenarios that ought to be discussed in the public realm, e.g., a future when we learn to live with frequent cyber security incidents or a future when we decide to future-proof smart devices at the expense of adoption timelines (Michalec, 2022).

- **Smart devices pose novel privacy risks due to the volume and granularity of data leading to novel market analytics**. This creates disproportionate impacts on marginalised and vulnerable groups (e.g., victims of domestic abuse, children and the elderly, those in disadvantaged socio-economic settings). Commercial actors are now able collect data about data subjects at unprecedented granularity (Christianson, 2013; Shaw et al., 2022). This leads to the following privacy risks: Inference of sensitive information, discriminative customer segmentation (e.g., unfavourable energy tariffs based on smart meter data), multi-person data (e.g., a situation when an individual cannot give consent to give out personal data if living in shared spaces), Data aggregation (e.g., the unpredictability resulting from combining analytics from multiple sources which makes it impossible to inform data subjects about potential future insights and uses of their data) (Veliz and Grunewald, 2018).
- They created a **new regime of governance through testing** (Marres and Stark, 2020; Michalec et al., 2020). From smart energy trials to self-driving vehicles testing, experimentation in the society is now ubiquitous. This process is much more than merely producing test results. Testing is generative in itself; expert-led testing deliberately introduces something new into society (Marres and Stark, 2020). The explicit goal of testbeds for innovations in smart energy or mobility to get technologies market-ready as soon as possible.
- Past examples of delays and resistance in adoption of smart meters show that **we cannot take adoption and consumer engagement for granted**. Consumer apathy, mistrust and confusion about the stated benefits of smart meters led to a **costly delay in the implementation of smart grid** (Michalec et al., 2019; Sovacool et al., 2017)

With the demonstrated societal impact of smart technologies, it can be seen as an improvement over existing manual and non-smart systems. But this force for good would only be endearing if privacy, security as well as responsible innovation underlines its vision.

2. **Are there any groups in society who may particularly benefit from or be vulnerable to the increasing prevalence of smart technology, such as young or elderly people, people with disabilities and people likely to be digitally excluded?**

We would like to highlight the following vulnerable groups:

- **People experiencing domestic violence** are increasingly being surveilled and controlled by abusers via technology. The usability of devices, with respect to understanding and negating such control is still not optimum (Parkin et al., 2019).
- **Less digitally literate users** as vulnerable to over- or under-trusting of AI systems based on a lack of technical understanding (Hoffman et al., 2018).
- **People without internet access who rely on the provision of public services** (e.g., education, benefits, online payments).
- **Children** who use devices that are connected to the internet. Smart toys pose real security and privacy threats, including the transmission of imagery and audio over unprotected channels (Quayyum, 2021).
- **Refugee and asylum seeker communities** who rely on digital public services for the provision of necessities

- **People in disadvantaged socio-economic setting** who have to give up their data to obtain benefits and other public services

Additionally, we would like to stress that identifying vulnerable users might become increasingly challenging as smart technologies proliferate. Understanding barriers or a lack of access becomes challenging when millions of people use a specific technology. Overall, there needs to be an evaluation of what real opportunities people have when accessing smart systems. This evaluation framework ought to move beyond usability considerations and include accessibility, human capabilities and second order effects. This is because people affected by smart technologies are both active users, indirect users, and bystanders. While usability evaluations are often concerned with direct users the bystanders are not heard. In smart technology evaluations, we need to consider human diversity in terms of age, gender, ability, political and economic circumstances (Chowdhury et al. 2022).

3. **How can we incentivise or encourage design that is safe, secure, environmentally- and user-friendly and human rights compliant?**

We outline the following recommendations:

- Where possible, research funders should commission **evidence-based security evaluations** (in addition to the existing expertise-based evaluation and certification processes) would incentivise both 1) openness and transparency in design and development (currently disincentivised by expertise-based evaluation processes); and 2) building security evaluation capabilities into development-focused companies (by allowing companies to gain value from identifying security issues early in the design process). The current state of tooling is not appropriate for use by general designers and developers and requires further research and development (Dupressoir et al., 2021). It took 20 years for aviation regulators to accept formal and logical evidence as part of certification processes for safety-critical software in aviation; and it spurred research in a big way. We are recommending that “now” should be the start of those 20 years for security.
- **Smart device manufacturers and app developers need to focus on user safety** and engage more with the issues around technology misuse (Strohmayer et al., 2021).
- **The government ought to provide security and privacy principles that will help developers design and develop secure system that will also protect users’ their privacy**. There is a need to support developers or companies who are developing these systems (Ramokapane et al., 2022; Chowdhury, P.D. et al., 2021; Rashid, 2021; Patanik et al., 2021; Weyns et al., 2021)
- **Businesses need to understand how consumers use their technologies** as well as their expectations regarding security, privacy, and safety. This would help companies to build and implement relevant controls for users. (Abdi et al, 2021; Ramokapane et al., 2019a)
- **We encourage an inquiry into a design of automated privacy assistants that lay users could trust when managing their privacy online**. The users are expected to interact with a large number of IoT devices, and it is not always trivial to make informed decisions since many privacy situations may exist (e.g., purpose of the data collection, the retention period). The privacy assistants will play an important role in people’s lives

in the coming years, and recent work shows that the users are welcoming to use privacy assistants when some decisions are taken care of automatically (Colnago et al., 2020). Such AI-based privacy assistants could collaborate with humans to make sharing decisions (Kokciyan and Yolum, 2022).

- **The government ought to design frameworks to incentivise technology companies to effectively collaborate with researchers and share data** to support designs that are safe, secure, environmentally- and user-friendly and human rights compliant (OII, 2022). For example, the Online Safety Bill could provide concrete and enforceable mechanisms that enable UK platform users to freely share their data with independent scientists in a sensible, legal, and timely way. The Bill could also call for a new research framework for augmenting existing databanks and population studies with online platform data.
- **As smart technology enters the society, policy makers and developers must strive to build trust in the systems using either technical or social explainability, as appropriate.** This should occur only when the smart systems are actually trustworthy. By providing knowledge of the governing ecosystem, industries like aviation and engineering have built stable trust with everyday people who do not necessarily need to understand the technologies themselves (Giddens, 1990). This is known as "social explainability." We propose a parallel movement should occur in the field of smart technologies. We conducted a study that extended this concept to AI systems using a series of "social" explanations (based on external certification of the system, data security and privacy). Findings reveal that more technical information predicts higher trust from those with higher digital literacy, but those of lower digital literacy given purely technical explanations have the worst trust overall. For this group, social explainability works best (REPHRAIN, 2022).
- **Open source design and discussion forums**: It is important that the design of security and privacy algorithms is made public. Likewise, requests for comments from the community and experts ought to remain publicly available. A recent example is the standardisation process for lightweight cryptography that is suitable for constrained environments, IoT devices are an example of such systems (NIST LWC, 2021). LWC-forum is created to get comments from the experts and to open up the algorithms for rigorous testing and validation.
- **Development tools upgrade**: It is important that the government invests in the development of recent research-based proof of concepts for privacy and security and make those available for developers to deploy in IoT systems. A recent study on developers' understanding of the available solutions to security and privacy problems has revealed that the knowledge about novel approaches such as differential privacy and federated learning is lacking, and these ideas are currently challenging for developers implement (Tahaei, 2022).

4. **What are the key short- and long-term risks and threats, and how can we ensure the devices, systems and networks of individuals, businesses and organisations are digitally-literate and cyber secure?**

We outline the following risks and threats:

- **Lack of consent from the bystanders and indirect users.** Most IoT devices still rely on Terms of Service which are shown during setup to only the device owner, but anyone near an IoT device can use it. Anyone near an IoT device can also have their data collected by it. (Meng et al., 2021)
- **Smart energy systems can be misused and leave people without electricity.** It is also possible to exclude those from low socio-economic backgrounds because of how they use energy (Ramokapane et al., 2022). For example, consumers can be penalised (i.e., cut off from the grid or charged extra) for using certain appliances (e.g., washing machines) during peak hours. These providers can use energy data to profile users using the devices, the times they use electricity and the amount of energy they use. It is also possible that certain neighbourhoods (or houses) may be required to pay more for electricity than others (Jakobi et al., 2019).
- There is a possibility that **third parties accessing user data might deny people their services** (e.g., processing insurance claims based on social media data and cookies)
- The interactions with technology that directly lead to harm are unclear and, as with online harm more generally, suffer from a variety of **measurement inconsistencies** (Ellis, 2020).
- **Physical Attacks to IoT devices**: Common threats to IoT devices are hardware attacks. For example, “Dolphin Attack” injects inaudible commands on voice controllable systems (VCS), e.g., Siri (Zhang, 2017). Another similar attack uses laser signals to inject voice commands (Sugawara, 2020). Physical attacks can have consequences on safety, e.g., when an adversary remotely manipulates the temperature sensor measurements of an infant incubator to cause harm without tampering with the victim system or triggering automatic temperature alarms (Yazhou, 2019). Connected sensory systems being used in national critical infrastructure can result in physical damage to property and life of people (Ahmed et al., 2017).

We can ensure digital literacy and security in society through:

- **Providing usable security mechanisms especially during the set-up process**. (Ramokapane et al, 2019b)
- **Helping people to understand how their energy data might be misused** (Ramokapane et al., 2022)
- **Developing mechanisms that will allow users to understand smart home assistant** ecosystem and therefore make informed decisions on how they would want to use their smart home technologies. (Abdi et al., 2019)
- **Research aiming to understand how individuals and groups make decisions in relation to privacy and security in an everyday context.** These decisions happen rapidly and with little conscious awareness because they are habitual behaviours that are typically automatic (e.g., Shaw, Ellis and Ziegler, 2018).
- **Mandating no default credentials on IoT devices**: We recommend to assign each device a unique ID and password from the factory floor so making default random credentials rather than same (such as user:admin, password:admin) for all the devices.
- As physical cyberattacks become a novel threat, it is important to **validate the inputs into sensors and computing devices not only in the software layer but in the hardware layer** as well (Ahmed et al, 2021).

- **Effective security labelling**. Our rapid evidence assessment of labelling schemes (Blythe and Johnson, 2018) suggested that (e.g. nutrition or energy) labels are generally effective in influencing consumer and/or manufacturer behaviour but that the different types (e.g. seal of approval labels, graded labels) vary in the extent to which they are understood and the impacts they have on consumer behaviour. A number of biases (including the affect heuristic, whereby a consumer's attention is drawn to some but not all of the information they should consider) were also identified that can distort the effects of different types of labels, and backfire effects were identified for labels that have not been sufficiently tested prior to their use. Moreover, the complexity of measuring "security" and the fact that (unlike e.g., calorific content) the level of protection a device (or software) can provide will be dynamic (which might require a dynamic label). These issues should be attended to when designing security labels that aim to educate and nudge consumers.

5. **How will current geopolitical concerns influence domestic consumers, e.g. regarding standards of imported goods or in how we can deal with cyber threats?**

We call for increased international collaboration despite geopolitical concerns. In particular, we remark that:

- Dealing with cyber threats requires trustworthy infrastructure. The current complexity and our lack of understanding of core digital components—CPUs and SoCs—has led to serious security and privacy breaches in recent years. Recent efforts to develop open, simple and understandable hardware designs (RISC-V, 2022) with extensions focused on supporting the safe and secure implementation of cryptography and privacy-enhancing mechanisms (RISC-V Crypto ISE, see Github, 2022; CHERI RISC-V, see The University of Cambridge, 2022) is an opportunity to set new safety and security standards, especially in the domain of low-cost devices.
- Self-sovereignty in digital infrastructure is important, but insufficient. Global regulations and trust (even beyond international commitments such as the Paris Call for Trust and Security in Cyberspace (Ministry for Europe and Foreign Affairs, 2018) are required in order to allow the safe and secure trade of goods *and digital services* internationally. Vulnerabilities in devices manufactured, sold or used outside of Britain affects the security of digital assets in the UK, and makes the attribution (or even the detection) of state-level cyber-attacks difficult or impossible. Local technical solutions can help—especially in protecting the privacy and confidentiality of data (and, with a bit more effort, its integrity), and should be incentivised (as per Q3, including evidence-based evaluation frameworks facilitating international trades and services), but cannot be expected of global devices and services.
- International trust and transparency in cyber security matters can be facilitated, as is already done in space matters (Sharemind, 2015) through multi-party computation techniques. Bootstrapping trust in these techniques and their implementations can be done through machine-checked proofs, as in the ANALYSIS project, producing independently verifiable proof certificates as evidence of the security of protocols and implementations. Such proofs already exist for Yao's garbled circuits (Almeida et al.,

2017) for a simple MPC protocol based on arithmetic circuits (Haagh et al., 2018), and for the Goldreich, Micali and Widgerson general protocol (Morrisett et al., 2021).

6. **Do existing frameworks, like data protection legislation and the Public Security and Telecommunications Infrastructure Bill, adequately address concerns with smart technology, and if not, how could they be changed?**

We posit that the existing frameworks lag behind what is occurring in practice now, and what advancements are impending in IoT (e.g., in smart energy context) and smart wearables (e.g., head worn Augmented Reality (AR) devices). Below we outline the areas that require regulatory improvement as well as recommend regulatory mechanisms:

- Legal frameworks and laws are not well aligned with developers who have to implement them in code. In addition to such legislation **there needs to be guidance aimed at groups like developers** on how to practically implement what is being asked for. Possibly also a recognition of the role of platforms, like the Google Play store, and working to better integrate information about the laws such that developers understand what they are responsible for. (Tahaei et al., 2021 and 2020).
- **The lawful basis requirement for processing personal data is persistently under attack.** Consent can be readily garnered from the user through a variety of means e.g., dark patterns; incentivisation/coercion such as restricting services or capabilities without consent; exploiting user apathy to agree to terms etc. It is also feasible to argue for "legitimate interest" in capture and processing, or if well-resourced the activities can simply be pursued regardless, in the knowledge this risks fines further down the line.
- **The scope of what data is captured, and what resultant insights can be inferred from said data (computed or processed data), is continually increasing**, driven by local and cloud-based machine learning. For example, take basic IoT such as smart speakers - even a short voice interaction can be used to infer much about the user, for example affective state, personal characteristics such as gender and age etc. (Kwasny and Hemmerling, 2021). These insights can also be retroactively applied, depending on the retention policies employed. Consequently, the definitions of special category data such as in GDPR are insufficient in addressing what captured data can potentially reveal given further processing/inference. This situation is only likely to get worse - quite dramatically so if we see consumer XR see significant adoption (McGill, 2021), and the scope of what is longitudinally revealed by captured data hinders any kind of meaningful disclosure to users.
- **The data subject is now no longer restricted to the user or device owner -** bystanders to IoT and smart technology are subject to data capture without consent based on legitimate interest.
- The companies behind many of IoT systems often undertake design and development in countries with less privacy protections enshrined in law - consequently **privacy by design, and ground-up consideration of GDPR, ePrivacy etc. is undermined,** and later efforts to force compliance encounter consumer backlashes under suggestions products might be withdrawn
- The current frameworks do not sufficiently address the user data concerns with smart technology. These frameworks need to integrate privacy and transparency requirements that helps developers and domain experts addressing user data concerns which when

implemented will also increase user trust in the software and the technology. (Zieni, Heckel 2021, Zieni et al. 2021)

- The immaturity of the existing IoT security frameworks led to **low public security awareness and poor quality of security labelling.** In Blythe et al. (2019) we compiled a database of 270 consumer IoT devices produced by 220 different manufacturers on sale at the time of the study. Our findings suggest that manufacturers provide too little publicly available information about the security features of their devices, which makes market surveillance challenging and provides consumers with little information about the security of devices before their purchase. For example, for none of the devices examined was information provided about the period over which security updates would be provided. For only 20% of devices were Wi-Fi encryption standards discussed, and in only 10% were features designed to protect the privacy of users discussed.

REFERENCES

Abdi, N., Ramokapane, K. M., & Such, J. M. (2019). More than smart speakers: security and privacy perceptions of smart home personal assistants. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)* (pp. 451-466).

Abdi, N., Zhan, X., Ramokapane, K. M., & Such, J. (2021). Privacy norms for smart home personal assistants. In *Proceedings of the 2021 CHI conference on human factors in computing systems* (pp. 1-14).

Ahmed, C. M., MR, G. R., & Mathur, A. P. (2020, October). Challenges in machine learning based approaches for real-time anomaly detection in industrial control systems. In *Proceedings of the 6th ACM on cyber-physical system security workshop* (pp. 23-29).

Ahmed, C. M., Mathur, A., & Ochoa, M. (2017). NoiSense: Detecting data integrity attacks on sensor measurements using hardware-based fingerprints. *arXiv preprint arXiv:1712.01598*.

Almeida, J.B., Barbosa, M., Barthe, G., Dupressoir, F., Grégoire, B., Laporte, V., and Pereira, V. (2017) A Fast and Verified Software Stack for Secure Function Evaluation. *CCS 2017:* 1989-2006

Anderson, R. (2018) Making security sustainable. *Communications of the ACM* 61.3: 24-26.

Blythe, J. M., & Johnson, S. D. (2018). Rapid evidence assessment on labelling schemes and implications for consumer IoT security. Department for Digital, Culture, Media and Sport, https://www.gov.uk/government/publications/rapid-evidence-assessment-on-labelling-schemes-for-iot-security.

Blythe, J. M., Sombatruang, N., & Johnson, S. D. (2019). What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages?. Journal of Cybersecurity, 5(1), https://academic.oup.com/cybersecurity/article/5/1/tyz005/5519411?searchresult=1.

Chowdhury, P. D., Hallett, J., Patnaik, N., Tahaei, M., & Rashid, A. (2021, October). Developers Are Neither Enemies Nor Users: They Are Collaborators. In *2021 IEEE Secure Development Conference (SecDev)* (pp. 47-55). IEEE.

Chowdhury, P. D., Dominguez, A., Ramokapane, M. K., & Rashid, A. (2022). The Political Economy of Privacy Enhancing Technologies. *arXiv preprint arXiv:2202.08548*.

Christianson, B. (2013) Living in an impossible world. Philosophy and Technology, 26(4):411{429}

Colnago, J., Feng, Y., Palanivel, T., Pearman, S., Ung, M., Acquisti, A., Cranor, L.F. and Sadeh, N. (2020) Informing the Design of a Personalized Privacy Assistant for the Internet of Things. Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. Association for Computing Machinery, New York, NY, USA, 1–13.

Davidson, B., Ellis, D., Stachl, C., Taylor, P., & Joinson, A. (2022). Measurement practices exacerbate the generalizability crisis: Novel digital measures can help. *Behavioural and Brain Sciences, 45*, E10. doi:10.1017/S0140525X21000534

Ellis, D. A. (2020). *Smartphones within psychological science*. Cambridge University Press.

Giddens, A. (1990) A. Giddens. The consequences of modernity. Oxford, Polity Press, 1:1–19, 1990.

Github (2022) RISC-V Crypto ISE https://github.com/scarv/xcrypto

Golomb, S.W. (1971) Mathematical models: Uses and limitations. *IEEE Transactions on Reliability* 20.3. 130-131

Haagh, H., Karbyshev, A. Oechsner, S., Spitters, B., Strub, P.Y. (2018) Computer-Aided Proofs for Multiparty Computation with Active Security. *CSF 2018:* 119-131

Kokciyan, N. and Yolum, P. (2022) Taking Situation-Based Privacy Decisions: Privacy Assistants Working with Humans. In Proceedings of the 31st International Joint Conference on Artificial Intelligence and the 25th European Conference on Artificial Intelligence (IJCAI-ECAI) [to appear].

Jakobi, T., Patil, S., Randall, D., Stevens, G., and Wulf, V. (2019) It Is About What They Could Do with the Data: A User Perspective on Privacy in Smart Metering. *ACM Trans. Comput.-Hum. Interact*. 26, 1, Article 2, 44 pages.

Kwasny, D., & Hemmerling, D. (2021). Gender and age estimation methods based on speech using deep neural networks. Sensors, 21(14), 4785.

Marres, N., & Stark, D. (2020). Put to the test: For a new sociology of testing. *The British Journal of Sociology*, *71*(3), 423-443.

McGill; Mark, "The IEEE Global Initiative on Ethics of Extended Reality (XR) Report--Extended Reality (XR) and the Erosion of Anonymity and Privacy," in Extended Reality (XR) and the Erosion of Anonymity and Privacy - White Paper , vol., no., pp.1-24, 18 Nov. 2021.

McQueenie, R., Ellis, D. A., Fleming, M., Wilson, P., & Williamson, A. E. (2021). Educational associations with missed GP appointments for patients under 35 years old: administrative data linkage study. *BMC Medicine*, *19*(1), 1-7.

Meng, N., Keküllüoğlu, D., Vaniea, K. (2021) Owning and Sharing: Privacy Perceptions of Smart Speaker Users. *Proceedings of the ACM Conference on Computer Supported Cooperative Work and Social Computing.* https://groups.inf.ed.ac.uk/tulips/papers/meng2021cscw.pdf

Michalec, O., Hayes, E.; Longhurst, J. and Tudgey, D. (2019) Exploring the potential and communication of metering in the energy and water sectors. Utilities Policy. Available here

Michalec, O., O'Donovan, C. & Sobhani, M. (2021) What is robotics made of? The interdisciplinary politics of robotics research. *Humanit Soc Sci Commun* **8,** 65. https://doi.org/10.1057/s41599-021-00737-6

Michalec, O., Milyaeva, S. and Rashid, A (2022) When the future meets the past: can safety and cyber security coexist in modern critical infrastructures? Big Data and Society (In press)

Michalec, O. and Chitchyan, R. (2022) Smart Lens project https://www.bristol.ac.uk/bristol-digital-futures-institute/research/seed-corn-funding/energy-systems/get-a-smart-meter/#d.en.577338

Michalec, O. (2022) How to Talk about Cybersecurity of Emerging Technologies A Report to Board Level Executives in the Energy Sector. Policy briefing https://petras-iot.org/wp-content/uploads/2022/03/How-to-talk-about-cybersecurity-of-emerging-technologies.pdf

Ministry for Europe and Foreign Affairs (France) (2018) Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in

Morrisett, G., Shi, E., Sojakova, K., Fan, X., Gancher, J. (2021) IPDL: A Simple Framework for Formally Verifying Distributed Cryptographic Protocols. *IACR Cryptol. ePrint Arch.* 2021: 147

NIST LWC (2021). Lightweight Cryptography, url: https://csrc.nist.gov/Projects/lightweight-cryptography last accessed: 20th June 2022.

The Oxford Internet Institute (OII) (2022) An open letter to Mark Zuckerberg https://www.oii.ox.ac.uk/an-open-letter-to-mark-zuckerberg/#contributors

Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, *30*, 100343.

Parkin, S., Patel, T., Lopez-Neira, I. and Tanczer, L. (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 (NSPW '19). Association for Computing Machinery, New York, NY, USA, 1–15. https://doi.org/10.1145/3368860.3368861

Patnaik, N., Dwyer, A. C., Hallett, J., & Rashid, A. (2021). Don't forget your classics: Systematizing 45 years of Ancestry for Security API Usability Recommendations. *arXiv preprint arXiv:2105.02031*.

Privacy International (2021) Best Before date policy brief: Device sustainability through long-term software support https://privacyinternational.org/advocacy/4636/best-date-policy-brief-device-sustainability-through-long-term-software-support

Ramokapane, K. M., van der Linden, D., & Zamansky, A. (2019a). Does my dog really need a gadget? What can we learn from pet owners' motivations for using pet wearables?. In *Proceedings of the Sixth International Conference on Animal-Computer Interaction* (pp. 1-6).

Ramokapane, K. M., Mazeli, A. C., & Rashid, A. (2019b). Skip, Skip, Skip, Accept!!!: A Study on the Usability of Smartphone Manufacturer Provided Default Features and User Privacy. *Proc. Priv. Enhancing Technol.*, *2019*(2), 209-227.

Ramokapane, K. M., Bird, C., Rashid, A., & Chitchyan, R. (2022). Privacy Design Strategies for Home Energy Management Systems (HEMS). In *CHI Conference on Human Factors in Computing Systems* (pp. 1-15).

Rashid, A. (2021). Developer-Centred Security. In *Encyclopedia of Cryptography, Security and Privacy*. Springer.

RISC-V (2022) RISC-V Announces First New Specifications of 2022, Adding to 16 Ratified in 2021 | RISC-V International. Community news https://riscv.org/

REPHRAIN (2022) SOXAI – Social Explainability for trustworthy AI: What types of explanations can help users develop appropriate trust? https://www.rephrain.ac.uk/soxai/

Sharemind (2015) Using Sharemind to Estimate Satellite Collision Probability https://sharemind.cyber.ee/satellite-collision-security/

Shaw, H., Ellis, D. A., & Ziegler, F. V. (2018). The Technology Integration Model (TIM). Predicting the continued use of technology. *Computers in Human Behaviour, 83*, 204-214.

Shaw, H., Taylor, P. J., Ellis, D. A., & Conchie, S. M. (2022). Behavioural consistency in the digital age. *Psychological science, 33*(3), 364-370.

Sovacool, B. K., Kivimaa, P., Hielscher, S., & Jenkins, K. (2017). Vulnerability and resistance in the United Kingdom's smart meter transition. *Energy Policy*, *109*, 767-781.

Strohmayer, A., Slupska, J., Bellini, R., Coventry, L., Hairston, T., & Dodge, A. (2021). Trust and Abusability Toolkit: Centering Safety in Human-Data Interactions. Northumbria University

Sugawara, T., Cyr, B., Rampazzi, S., Genkin, D., & Fu, K. (2020). Light Commands:{Laser-Based} Audio Injection Attacks on {Voice-Controllable} Systems. In *29th USENIX Security Symposium (USENIX Security 20)* (pp. 2631-2648).

The University of Cambridge (2022) CHERI RISC-V https://www.cl.cam.ac.uk/research/security/ctsrd/cheri/cheri-risc-v.html

Tahaei, M., Vaniea, K., and Saphra, N. (2020) Understanding Privacy-Related Questions on Stack Overflow. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.*

Tahaei, M., Frik, A., and Vaniea, K. (2021) Privacy Champions in Software Teams: Understanding Their Motivations, Strategies, and Challenges. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*.

Tahaei, M., Li, T., & Vaniea, K. (2022). Understanding Privacy-Related Advice on Stack Overflow. *Proc. Priv. Enhancing Technol.*, *2022*(2), 114-131.

Tu, Y., Rampazzi, S., Hao, B., Rodriguez, A., Fu, K., & Hei, X. (2019). Trick or heat? Manipulating critical temperature-based control systems using rectification attacks. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (pp. 2301-2315).

Weyns, D., Bures, T., Calinescu, R., Craggs, B., Fitzgerald, J., Garlan, D., ... & Schmerl, B. (2021, September). Six Software Engineering Principles for Smarter Cyber-Physical Systems. In *2021 IEEE International Conference on Autonomic Computing and Self-Organizing Systems Companion (ACSOS-C)* (pp. 198-203). IEEE.

Zhang, G., Yan, C., Ji, X., Zhang, T., Zhang, T., & Xu, W. (2017). Dolphinattack: Inaudible voice commands. In *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security* (pp. 103-117).

Zieni, B. and Heckel, R. (2021) TEM: A Transparency Engineering Methodology Enabling Users' Trust Judgement. *2021 IEEE 29th International Requirements Engineering Conference (RE),* pp. 94-105, doi: 10.1109/RE51729.2021.00016.

Zieni, B., Spagnuelo, D., & Heckel, R. (2021) Transparency by default: GDPR Patterns for Agile Development. In *International Conference on Electronic Government and the Information Systems Perspective* (pp. 89-102). Springer, Cham.