Written evidence submitted by Professor George Loukas, Professor Mina Vasalou and Dr Laura Benton

Authors:

Prof. George Loukas, Professor of Cyber Security, Head of IoT and Security (ISEC) Research Centre, University of Greenwich [https://www.gre.ac.uk/people/rep/las/george-loukas]

Prof. Mina Vasalou, Professor of Interaction Design, UCL Knowledge Lab, University College London [https://iris.ucl.ac.uk/iris/browse/profile?upi=MVASA31]

Dr Laura Benton, Senior Research Associate, UCL Knowledge Lab, University College London [https://iris.ucl.ac.uk/iris/browse/profile?upi=LBENT04]

About the Authors:

Professor Loukas specialises in protecting systems from cyber security breaches that have physical impact, including smart devices used in domestic, industrial and commercial environments. He has previously led five national and international projects and is on the editorial board of the flagship IEEE Transactions in Information Forensics and Security journal. He is currently leading the ISEC research centre with 27 members focusing on Internet of Things and Security and the £2.4M EPSRC CHAI project, which brings together diverse expertise from Greenwich, UCL, Reading, Queen Mary and Bristol University in extending cyber hygiene to AI-enabled smart home environments.

Professor Vasalou and **Dr Benton** are part of the UCL Knowledge Lab (UCLKL) at IOE, UCL's Faculty of Education and Society, rated number 1 for the strength of its research in REF2021. The mission of the UCLKL is to explore how we live and learn with technology and media to solve societal challenges. Researchers within the lab design and evaluate digital innovations and research learning and social practice in the digital world with stakeholders across the public and private sector. Professor Vasalou recently led the 4.5 year €5.5m H2020 iRead project, which received a quality mark from the DfE's Hungry Little Minds campaign. Both Professor Vasalou and Dr Benton have extensive expertise in collaborating with diverse and vulnerable users through the design of new digital technologies from their work over the past decade, and are currently leading on the design of a new smart device security training programme as part of the CHAI project.

Executive Summary:

1. We are submitting this evidence with a particular focus on the specific risks raised by AI-enabled smart devices and smart device users in a social housing context. This evidence is primarily based on novel research undertaken as part of the £2.4M EPSRC CHAI project[1] which is focused on how to support domestic users of AI-enabled smart devices living in social housing to better protect themselves against potential cyberattacks. It is also based on novel research carried out as part of the £1M CHIST-ERA Cocoon project[2], which focused on user-centric cyber security in smart homes. We address two of the questions from the call in this context, which we summarise below.

2. *Are there any groups in society who may particularly benefit from or be vulnerable to the increasing prevalence of smart technology?* Our evidence shows that smart devices can offer a number of benefits to people living in social housing and housing providers are beginning to pilot these devices in homes, but this is also a group who can be extremely vulnerable in the event of a cybersecurity breach with particular concerns around single women and girls as well as those are who have a history or increased likelihood of experiencing mental health issues. There is currently limited experience, expertise and available support related to the security of smart devices amongst both housing providers and social housing residents. We offer guidance for

[1] https://www.project-chai.org
[2] https://cocoon-project.eu

housing providers looking to install smart devices on how to be open and transparent about tenant risk, rights and personal data use (see paragraph 15).

3. *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?* Our evidence shows that smart devices containing AI functionality in particular need to be carefully designed to ensure they are safe and secure for use within the home because people find it difficult to notice security breaches on these devices and any attacks can have considerable emotional impact on them, potentially exacerbating existing mental health difficulties. We have also identified a lack of adequate guidance around preventing and mitigating attacks, with existing cyber hygiene guidelines for smart AI-enabled environments not fit for purpose having insufficient existing scientific evidence for public recommendation. We offer recommendations for smart technology providers by extending the Code of Practice for Consumer IoT products to include support for users to prevent security breaches in AI-enabled devices as well as recognise and respond to a breach (see paragraph 14).

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?

Drivers for smart technology in the social housing sector

4. There are currently 4 million households living in social housing in England alone. A quarter of this population are aged over 65, a third have dependent children and over half of the householders include someone with a long-term illness or disability, and as a whole this is a group that includes some of the most vulnerable people in society[3].

5. Currently social housing providers are focused on piloting smart devices in a small number of their tenants' homes that can facilitate the monitoring and maintenance of homes (for example smart smoke alarms, sensors and thermostats). Whilst most are yet to proceed with widespread rollouts of these devices, it is expected in the coming years this will increase significantly.

6. The variety of potential benefits for both the landlord and the tenant have been highlighted by many industry experts, which include offering a cost-effective way for housing providers to meet expected housing standards (e.g. by identifying potential disrepair issues earlier) and increased empowerment and equality for the tenant[4].

Security breaches and their impact on social housing residents' wellbeing

7. There has been little consideration given to the additional safety and security risks these devices may introduce within already vulnerable households, which is of particular concern in cases where tenants feel they have little choice in whether to have a particular device installed in their home or they move into a property which already has smart devices installed and are unequipped to deal with potential associated security threats.

8. In our work we have interviewed (i) social housing providers looking to implement smart devices in their properties, (ii) specialists in national housing policy and regulation as well as (iii) a range of social housing tenants from 18-64, many of whom are living with conditions such as cerebral palsy, hearing impairments, autism, anorexia as well as a rare brain disorder.

---

[3] English Housing Survey 2020 to 2021: headline report https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1060141/2020-21_EHS_Headline_Report_revised.pdf

[4] HACT White Paper series (2020) Do the smart thing: The future of the social smart home https://hact.org.uk/nextinnovations/smart-homes/

9. Our research shows that social housing providers are looking at introducing smart thermostats and sensors which can offer them a range as benefits including monitoring the state of a property, identifying tenants at risk of fuel poverty and potentially supporting tenants to heat their homes in more efficient ways.

10. Tenants report concerns if smart devices were to be hacked. For instance, many people have concerns about any smart devices which have the potential to access financial information, particularly around financial data that could impact their ability (or not) to access benefits. Although the collection of in-home sensor data may seem innocuous, the use of AI within some of these devices allows many inferences to be made about the use and state of the property which could result in knowledge about when a property is typically empty, evidence to indicate a breach of tenancy agreement, blame apportioned for property disrepairs or becoming a target for firms looking to bring disrepairs cases against housing providers. Some tenants identify as particularly vulnerable (e.g., elderly, disabled) in the event of a breach that disrupts the functionality of a smart device, i.e. not having heating in the case of the smart thermostat. Single women living alone feel particularly vulnerable about a data breach allowing them to be identified, which could be especially problematic in cases where for instance a resident has been moved due to anti-social behaviour issues. Residents vary in their trust toward their housing providers' intentions and technical competence to install appropriate security, provide the required support and suitably manage the transition of residents within a property in relation to smart devices.

11. The concerns above are augmented by the difficulty people have to notice security breaches in smart technology. In traditional computing, such as emails and social media, people are generally more able than not to identify that they are under attack[5]. This is not the case with smart technology. Our 3-month long experiment involving 16 households and 29 people asked residents to first familiarise themselves with a set of smart home devices and then report when they thought they were under cyberattack. People had great difficulty ascribing the right cause to the attacks and distinguishing them from other irregularities naturally exhibited by the devices. Out of the 14 attacks launched, only 7 were reported by at least one of the 29 persons, while 24% of all incident reports were misidentified as natural glitches of the device[6].

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?

Short and long term risks and threats

12. As reported under (10) tenants of social housing identify risks related to smart technology namely *financial fraud, disruption of key services that they rely on and physical safety*. Additionally other research with residents mapped out a process that links the occurrence of a cybersecurity breach with the risk of long-term mental health effects[7]. People with intense emotional reactions, fight/flight action tendencies, and salient affective components experience the situation as emotionally highly relevant, but tend to react in a way that does not resolve the challenges created, which sets the stage for mental health risks.

---

[5] Heartfield, R. and Loukas, G., 2018. Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework. Computers & Security, 76, pp.101-127.

[6] Huijts, N., Haans, A., Budimir, S., Fontaine, J., Loukas, G., Roesch, E., Bezemski, A., Oostveen, A.M. and IJsselsteijn, W., 2019, March. Users' perceptions and responses to cyber-physical attacks on IoT devices in the home environment: a naturalistic field experiment. In *Society for Risk Analysis Benelux Conference: Reasoning with uncertainty*.

[7] Budimir, S., Fontaine, J.R., Huijts, N.M., Haans, A., Loukas, G. and Roesch, E.B., 2021. Emotional reactions to cybersecurity breach situations: Scenario-based survey study. Journal of medical Internet research, 23(5), p.e24879.

State of the art digital literacy for security is lacking

13. In our research we are focusing on the latest types of smart home devices which, in addition to smart connectivity, are also dependent on AI. As part of this work, we have studied the applicability of *cyber hygiene*, which is the collective name used for simple digital literacy guidelines for safe use of computing systems. Simple guidelines such as “don’t use the same password on multiple websites” or “check the sender’s email address” constitute a common and effective means for threat prevention in traditional computing practice, such as visiting social media or opening emails on PCs, laptops and mobile devices. We identified 105 guidelines are identified for helping users prevent Internet of Things (IoT) cyber security breaches, recommended by public authorities in the UK and abroad (e.g. NCSC, ENISA, ACSC, CISA and CAC) and other relevant institutions. We then evaluated their applicability on a representative set of currently available AI-enabled IoT devices, as well as their practicality. The outcome was a set of 75 guidelines that can be practical in terms of the effort and knowledge they require. The final step was to assess the scientific support that these guidelines have in the literature, scoring them in terms of the standing of the scientific venue where any support for them was published as well as the strength of the evidence provided. Out of the 75 potentially practical guidelines, only 5 were directly supported by strong scientific evidence (published in top venues and directly proven analytically or experimentally). Therefore, **most current cyber hygiene guidelines are not yet fit for purpose** for recommending to citizens interacting with AI-enabled smart environments. As cyber hygiene guidelines published on public institutions’ websites is a primary output of their digital literacy programmes, this shows an important deficit in current digital literacy efforts for smart technology.

Guidance for ensuring the devices, systems and networks of individuals, businesses and organisations are digitally-literate and cyber secure

Building on points 10-13, we draw implications for businesses and organisations that design/deploy smart technology in the home.

Recommendations for technology developers designing smart devices for the home

14. We recommend an extension of the Code of Practice for Consumer IoT Products (published in the government’s Secure by Design report). The extension should (i) provide the user with tools to prevent security breaches and (ii) help the user recognise and respond when their device’s security may have been breached via the following:
    - 14.1. **Strengthen the evidence base:** carry out research for evaluating the scientific strength of existing or new cyber hygiene guidelines for users of smart technology, which will complement the research already carried out for guidelines to smart technology developers. Recommending guidelines that are scientifically substantiated will be a vital block for any future digital literacy effort for users of smart technology. It will also minimise the risk of financial or other damage by following ineffective guidelines.
    - 14.2. **Adapt and incorporate familiar security features:** include security features that users are already familiar with from other devices connected to the internet e.g., multi-factor authentication and automatic security updates. This will ensure there is transferability with existing user habits.
    - 14.3. **Increasing device status visibility:** Use indicators such as lights, covers or sounds that alert users to the status of the device and whether it is recording data at that time, thus providing more control.
    - 14.4. **Explainability of AI**: Providing a user-friendly explanation of any decisions that a device’s AI has taken, so that the user can be better informed when the AI misbehaves.
    - 14.5. **Communicating cyber risks:** Manufacturers to acknowledge cyber risks in their devices’ manuals and to provide the user with basic actions to respond to a small set of possible cyber-related failures. This would be akin to current practice on basic faults provided in the manuals of white goods.
    - 14.6. **Providing emotional support**: Developing guidance for practitioners providing emotional support to victims of cyber attacks on smart technology more widely and beyond the current guidance which is focused on preventing “domestic cyber crime”.

Recommendations for housing providers deploying smart devices in social housing

15. We offer recommendations for housing providing planning to deploy smart devices in their properties to be open and transparent about tenants' risk, rights and personal data use in the following ways:
    15.1. Being transparent with residents about the **benefits and risks of introducing a new smart device** into a property to enable residents to assess these within their own personal circumstances before choosing to have a device installed.
    15.2. Ensure residents fully understand their rights around the **storage, use and sharing of personal data** collected from such devices.
    15.3. Provide a **simple explanation of any AI functionality** within a smart device.
    15.4. Offer residents suitable **training and support** when a new smart device is introduced into a property which should include a cybersecurity component.
    15.5. Ensure appropriate in-house (or externally bought in) smart device **cybersecurity expertise** within the organisation who can independently assess the risks of introducing a new smart device within tenant properties.