Institution: University College London

Unit of Assessment: UoA 20 - Social Work and Social Policy

Title of case study: Digital technologies for societal security

Period when the underpinning research was undertaken: DATE 2017- 2020

Details of staff conducting the underpinning research from the submitting unit:

Name(s):	**Role(s) (e.g. job title):**	**Period(s) employed by submitting HEI:**
Prof Madeline Carr,	Professor	2017-present
Prof Shane Johnson,	Professor	2004-present
Dr Irina Brass,	Associate Professor	2016-present
Dr Leonie Tanczer,	Lecturer	2017-present
Dr Alex Chung	Honorary Lecturer	2017-present

Period when the claimed impact occurred: 2017-2020

Is this case study continued from a case study submitted in 2014? No

1. Summary of the impact (indicative maximum 100 words)

The research on Internet security and digital technologies led by UCL's Departments of Science, Technology, Engineering and Public Policy (**STEaPP**) & Security and Crime Science (**SCS**) showcases the local relevance and global reach of multidisciplinary research on public policy tools to mitigate digital technology-induced risks, instabilities and insecurities in society. Their interrelated research on the Internet of Things (**IoT**) and cybersecurity in the UK and Europe has led to changes and improvements in cybersecurity and IoT standards and policies, increased public awareness on gender and IoT challenges, and improvements in the manufacturing practices of IoT vendors and allied actors. Their action research on IoT security has engaged international, national and local policy-makers, frontline workers, law enforcement, charities, and small and medium enterprises (**SMEs**).

2. Underpinning research (indicative maximum 500 words)

Many Internet-connected devices sold on the market are not secure by design, having weak passwords, no software (security) updates, and offering weak/no encryption to store sensitive data. UCL STEaPP academics Prof Carr, and Drs Brass, Tanczer, and Chung led IoT-focussed research as part of the **PETRAS** IoT Hub, which is a 12-instiution UCL-led National Centre of Excellence. PETRAS focusses on critical Privacy, Ethics, Trust, Reliability and Security research in relation to IoT technologies. The research conducted by the Hub, which also part-funded work by Prof Johnson from UCL Security and Crime Science, is crucial to ensuring that technological advances in the IoT are developed and applied safely and securely for businesses and consumers. Research by STEaPP academics focusses upon three interrelated concerns: policy, standardisation and governance gaps in the development of the IoT (**R1, 2, 5**, **6**); mapping cybersecurity evidence (**R3**); and the impact of IoT usage in the home on gender-based domestic violence and abuse (**R4**, **R5**). STEaPP's academics utilised '**embedded research'** and **'action research'** methodologies, which centre upon collaboration with stakeholders to understand and define policy, standards, and technology governance problems pertaining to IoT security. This methodology engaged diverse stakeholders including SMEs and standards-making bodies (**R2**, **R5**), women's shelters and refuges (**R4**), and government agencies (**R3**) in the co-production of knowledge, informed research findings, and influenced guidance (**R2**, **R5**).

Policy, standardisation and governance gaps in the development of the Internet of Things: In the UK, there is currently no regulation regarding the security of the IoT and devices vary in terms of the protection they provide. Using large sample experimental surveys and econometric modelling, Prof Johnson's work has demonstrated that consumers, regardless of age, gender and other factors, care about IoT security and that they are willing to pay for it (**R6**). However, his team's systematic qualitative analysis of the materials provided by device manufacturers (for 270 IoT devices) showed that they communicate little/no information about the security their devices provide (**R6**). For example, none provided details of the period over which software security updates would be provided, and only 5% provided details of how data would be protected on the cloud. In concert, this creates an information asymmetry that impairs consumer choice, making it difficult for them to assess the security provided by a device and consequently to buy secure products. Dr Brass, UCL Associate Professor in Regulation, Innovation and Public Policy and Chair of the IoT Technical Committee at The British Standards Institution (**BSI** - the UK national standards body), carried out research on policy, standardisation and governance gaps in the development of the IoT. The research sought to acknowledge and address the lack of SME representation in standards-setting processes (**R1**, **R2** and **R5**) and the impact this has on IoT SME product and services development. Brass particularly focused on the role that technical and normative standards play in filling current regulatory gaps for emerging digital technologies (**R5**). Brass led research in collaboration with the BSI, focussing on challenges in mass-market consumer products and digital healthcare (**R1**, **R2**). Through systematic reviews of emerging standards, regulatory, and operational responses to increased IoT security threats and vulnerabilities, as well as through a workshop hosted by the BSI (led by Dr Brass) which brought together government representatives, standards-makers, IoT SMEs, retailers and consumer associations. The research findings were published in an open access White Paper entitled ‘Navigating and Informing the IoT Standards Landscape: A Guide for SMEs and Start-ups’ which provides practical advice on IoT standards for SMEs (**R2**).

Mapping cybersecurity evidence: The UK’s policy-making community faces challenges in interpreting, evaluating and understanding evidence about cybersecurity. Through action research into these and allied issues, collaborating with user communities, Prof Carr and Dr Chung have explored how policy-makers make decisions on threats, risks, mitigation, and consequences related to cybersecurity based on highly diverse or heterogeneous evidence sources (**R3**). Their research showed that the highly heterogeneous evidence base makes it: difficult for policy-makers: i) to find the right information as cybersecurity is decentralised and incorporated into other functions of government; ii) to assess what constitutes the right information, and; iii) to know what information is relevant. In a five-month project funded through the Research Institute in Sociotechnical Cyber Security (**RISCS**), Prof Carr and Dr Chung collaborated with the Department for Digital, Culture, Media & Sport (**DCMS**) and National Cyber Security Centre (**NCSC**) to co-produce an interactive map of the rapidly developing UK cybersecurity policy landscape (**R3**).

Gender, domestic abuse and the Internet of Things: The link between the IoT, gender and domestic abuse is a growing area of concern for policy and practice. Situated at the intersection of technology, security, and gender, STEaPP’s work on these issues is run through PETRAS IoT Research Hub by Dr Tanczer, in partnership with the London Violence against Women and Girls (**VAWG**) Consortium, and the digital charity, Privacy International. This action research involves all 29 women shelters and refuges in London, aiming to co-produce knowledge relevant for addressing domestic abuse related to the IoT such as infographics, guides and resource lists for the voluntary and statutory support sector (**A**). Dr Tanczer’s research also explores the understandings of technology-facilitated abuse by practitioners such as police officers, the impact on the victims who use charitable services, and censorship and surveillance in academia (**R4**). This research showcased that technology-enabled domestic abuse is on the rise, that support services face shortcomings in their ability to respond or advise on IoT-facilitated tech abuse and that such evolving abuse forms are not explicitly considered in risk assessments and safety plans for victims. Related research by Dr Tanczer, working with a group of STEaPP MPA students has explored personal data ownership and portability within the context of IoT and the EU’s General Data Protection Regulations (**GDPR**).

3. References to the research (indicative maximum of six references)

R1. Brass, I. and J. Sowell. (2020). Adaptive Governance of the Internet of Things: Coping with Emerging Risks. Regulation & Governance. Special Issue on The Governance of Emerging Disruptive Technologies. https://doi.org/10.1111/rego.12343

R2. Brass, I., Pothong, K., & Hasham, M. (2019). Navigating and Informing the IoT Standards Landscape: A Guide for SMEs and Start-ups. LONDON: British Standards Institution.

R3. Chung, A., Dawda, S., Shaikh, S., & Carr, M. (2019). ECSEPA Map: UK Cyber Security Policy Making Map [Digital scholarly resource]. Retrieved from https://www.riscs.org.uk/ecsepa-map/.

R4. Lopez-Neira, I., Patel, T., Parkin, S., Danezis, G., & Tanczer, L. (2019). "Internet of Things": How Abuse is Getting Smarter. Safe – The Domestic Abuse Quarterly, (63), 22-26.
R5. Tanczer, L. M., 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 The Past Present And Future Of Cybersecurity. Hoboken: Wiley-Blackwell.
R6. Blythe, J.M., Sombatruang, N. and 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. doi:10.1093/cybsec/tyz005
R7. Johnson, S. D., Blythe, J. M., Manning, M., & Wong, G. T. (2020). The impact of IoT security labelling on consumer product choice and willingness to pay. PloS one, 15(1), e0227800. doi:10.31235/osf.io/4yxp2

4. Details of the impact (indicative maximum 750 words)

Working directly with international, national and local policy-makers, frontline workers, law enforcement, charities, and small and medium enterprises (**SMEs**), interrelated research on the Internet of Things (IoT) and cybersecurity in the UK and Europe has led to important changes and improvements in cybersecurity and IoT standards and governance, increased public awareness of gender and IoT challenges, and improvements in the manufacturing practices of IoT vendors and allied actors. The impact has emerged from deliberate pathways to impact built into this research on digital policy and societal security, and it includes the following:

Establishing the need for regulation to secure the IoT

Johnson's team's work on consumer perceptions and information asymmetry in the market-place (**R6**) has had a fundamental impact on UK policy currently being developed to secure the IoT. [TEXT REMOVED FOR PUBLICATION]. For example, the team's academic publications and a rapid evidence review produced for DCMS, are discussed extensively in the Canadian Multi-stakeholder Group Process Reports – written by the Internet Society, Canadian Government, and the Canadian Internet Registration Authority (who manage Canadian internet domains) – which make recommendations for securing the IoT in Canada. Dr Brass, Prof Carr and Dr Tanczer were members of the DCMS expert advisory group, drawing on their body of research to inform the DCMS 'Code of Practice for consumer IoT security' (published 14 October 2018).

Improving SME's representation in IoT standards-setting processes

SMEs and start-ups have an essential role in the IoT industry landscape: developing, and delivering Internet-enabled devices to consumers, in a growing market worth an estimated $248billion worldwide. However, their voices have rarely been sufficiently reflected, or "heard and understood in formal standards-making processes" (**R2**). Dr Brass's research on policy, standardisation and governance gaps in the development of the Internet of Things sought to better understand the challenges faced by SMEs in engaging with IoT standards-making processes (**R1**, **R2**, **R5**). Although SMEs frequently adopt standards to ensure responsible business practice and consumer protection for their product line, they have traditionally been underrepresented in standards-making bodies, which directly impacts the inclusivity of standards-making processes, especially in high innovation section pertaining to the Internet and digital economy.

In 2017, Dr. Brass was elected chair of the IoT/1 Technical Committee for the British Standards Institution (**BSI**)**,** which she had previously joined on the basis of PETRAS IoT-focussed research (**R1**, **R2** and **R5**). In July 2018, Brass organised a BSI IoT/1 workshop entitled 'SMEs and Start-ups Operating in the IoT Space', which enabled 5 SMEs representing the consumer IoT domain and a representative of a leading trade association for small and medium manufacturers of domestic appliances to directly participate in dialogue surrounding standards-setting with stakeholders across the IoT ecosystem, including the Department for Digital, Culture, Media and Sport (**DCMS**). Following the workshop, three participating SMEs were engaged in the co-production of a BSI White Paper (**R2**), which was the first to acknowledge and address a lack of SME representation in the IoT standards-setting community, with a dedicated section reflecting contributing SMEs' priority areas for IoT standards development (**R2**, section 2). The BSI White Paper (**R2**) provided SMEs with access to an expert guide combining

PETRAS IoT primary research, BSI workshop-influenced dialogues, and BSI committee guidance, which together empower SMEs to navigate and inform IoT standards. The BSI had acknowledged SMEs as "a challenging group for the BSI to engage with – particularly in a fast-moving sector like the IoT", with BSI Head of Industry & Government stating that they "genuinely wanted to understand issues faced by SMEs" (**C**). Brass's 'embedded researcher' methodology was then extended for a collaboration between the BSI and UCL STEaPP in the delivery of the team project of a group of MPA (Master of Public Administration) in Digital Technologies and Policy students, in which students conducted participant observation in several standards-making committees, as well as interviews and surveys with several IoT SMEs. This led to (**R1**) and as the title of a BSI-published report on the student research partnership attested, 'Deepening BSI's knowledge of SME needs in the IoT Space'. The BSI confirmed "it can be difficult for us to engage with SMEs… and It really helped us that they were not [from the] BSI because it made the results more objective" (BSI Head of Industry & Government) (**C**).

Informing the professional practice of UK cybersecurity policy-makers

In advanced industrialised states, cybersecurity policy is complex and challenging to incorporate into existing governance structures as it permeates previously distinct departmental jurisdictions. In the UK, policy-makers lacked effective resources to: understand a cybersecurity landscape in which 'evidence can be contradictory, gathered selectively and/or carry specific agendas or goals which could reduce its rigour and reliability' (RISCS policy brief for ECSEPA) (**D**); know where within HMG colleagues are working on cybersecurity issues; enable effective evidence-based decision-making. The limitations this critical gap in resources placed upon knowledge sharing across HMG and local governments contrasted heavily with the UK Government's National Cyber Security Strategy, 2016-2021 which advocates "a single, joined-up approach to incident management, based on an improved understanding and awareness of the threat and actions being taken against [the UK]" (NCSS, p.42 of **E**). Prof Carr and Dr Chung's research addressed these issues, by co-producing an interactive map with key government agencies, including DCMS and the National Cyber Security Centre (NCSC). The map (**R3**) is available on the RISCS website (since 1 May 2019): its 2400 data points and 2000 active links to webpages have enabled policy-makers to locate where cybersecurity work is taking place. [TEXT REMOVED FOR PUBLICATION]. The map (**R3**) provides the detailed information necessary for key stakeholders to improve their strategies for handling the risks, threats, and mitigations related to cybersecurity in the UK. Prof Carr and Dr Chung engaged stakeholders at the forefront of UK cyber policy issues in the co-production of the map (**R3**) between Nov 2017 and the map's publication on 1st May 2019. Their 'Evaluating Cyber Security Evidence for Policy Advice (**ECSEPA**) Mapping validation workshop' (8 February 2019, in London) was attended by the Cabinet Office; DCMS; Foreign & Commonwealth Office (**FCO**); The Ministry of Housing, Communities and Local Government (**MHCLG**), and Her Majesty's Revenue and Customs (**HMRC**). HMG ministries and agencies subsequently received closed-door presentations and private previews. [TEXT REMOVED FOR PUBLICATION]. The MHCLG invited Prof Carr and Dr Chung and the ESCEPA team to present (**R3**) to cybersecurity policy and operations specialists working across HMG and local governments, at events organised as part of the UK National Cyber Security Programme. One event at St George's House, Windsor Castle (10-11 June 2019) resulted in Prof Carr and Dr Chung co-authoring a joint publication summarising the "detailed discussions' of 'international importance" (St. George's Programme Director in (**F**)).

Informing policy-makers', professionals', & public understanding of IoT-facilitated abuse

IoT-enabled devices (e.g. Amazon's Alexa, Apple's Siri and Google Home, to smart light bulbs, kettles, security cameras and thermostats, etc,) are increasingly commonplace in domestic environments, with an estimated 22Billion IoT-connected devices in use at the end of 2018. However, the technological features (sensors, microphones, wireless connections etc.) at the core of their design also provide new avenues for domestic abuse. In Jan 2020, Refuge reported 72% of service users experienced abuse through technology (**L**). Policy-makers' and charities professionals' understanding of IoT-facilitated abuse is essential to ensure that legal dialogue is responsive to victims' needs, and appropriate support can be provided. Dr. Tanczer's research (**R4** & **R5**) and engagement with policy-makers such as DCMS and the UK Home Office via the Gender IoT project (**G-IoT**) has introduced IoT-facilitated abuse into political discourse in the UK, leading to: a parliamentary question on the issue (from Darren Jones) and 5 written questions being tabled to 3 different Government departments relating to data ownership and portability (by Lord Fox, and Lord Clement-Jones, July-August 2020) (**H**); and 2 POST Notes (on Cybersecurity and Consumer Devices' and Stalking and Harassment) citing5 of Dr Tanczer's publications to highlight concerns that IoT connected devices could enable domestic abuse [including **R4**, **R5**] (**H**). Dr. Tanczer briefed the Domestic Abuse Commissioner at the 'Internet of Things (IoT): Hidden Harms Summit' in April 2020 (invitation email provided, evidence **I**). Dr. Tanczer's collaboration with the London VAWG Consortium (relating to **R4**) has informed charity guidelines, training, and professional practice to support domestic abuse victims. For instance, the National Cybersecurity Centre developed tech abuse guidance based on Dr Tanczer's work (**J**). Dr Tanczer's research has been cited in charities' practitioner documents including the **AVA** (Against Violence and Abuse) Good Practice Briefing: Technology and Violence Against Women and G-IoT project resources have been referenced in publications from charities including the Latin American Women's Rights Service (**K**). Since 2018, Dr Tanczer has drawn on (**R4 & R5**) to provide training sessions to improve practitioners' understanding of the emergent threat of IoT technologies in domestic abuse, including for: Respect; Equation; AVA; and Hackney Council's Domestic Abuse Intervention Service [see 'statements' in **K**]. National media in the UK have widely quoted Dr. Tanczer to inform the public of IoT-facilitated abuse, including: the BBC ["How your Smart home Devices Can be turned against you" 12th May 2020, on the BBC Future website which boasts 3,900,000 unique browsers and 7,100,000 million page views per month]; and The Evening Standard [who profiled Dr. Tanczer in "The Progress 1000: London's most influential people 2019 – Technology: Cyber Security" on 2nd October 2019] (**G**).

5. Sources to corroborate the impfact (indicative maximum of 10 references)

A. Material co-produced (with London VAWG Consortium): Tech Abuse & IoT Guides https://bit.ly/3bRQoUm and https://bit.ly/3lj7rSd; G-IoT Resource List: https://bit.ly/3llRDOo.
B: [TEXT REMOVED FOR PUBLICATION]
C: Testimonial: BSI Head of Industry & Government [Available on request]
D: RISCS Policy Brief for ECSEPA: https://bit.ly/2OXqpln.
E: National Cyber Security Strategy, 2016-2021 (p.42): https://bit.ly/2PSczkv
F: St. George's House consultation: https://bit.ly/3rSj459 (quote, p1., ESCEPA case, p.17)
G: Refuge report: https://bit.ly/3vs7vnb & Media articles: Prof Tanczer feature in **'**Evening Standard' [02 October 2019]: https://bit.ly/3ljTdjW; 'BBC Future' [12 May 2020]; https://bbc.in/2OUnAkT. 'BBC Future' readership figures: https://bit.ly/3eEFrHq.
H: Parliamentary question; Darren Jones MP; Written questions: Lord Fox; Lord Clement-Jones); POSTnotes (593; pp.1–6): https://bit.ly/3ePBVKa; (592; pp.1–4),: https://bit.ly/3liSNdA
I: Emailed invitation for Prof Tanczer to brief the Domestic Abuse Commissioner (3 Sep 2020).
J: National Cyber Security Centre guidance: Domestic abuse and stalking: cybersecurity guidance for practitioners [TEXT REMOVED FOR PUBLICATION]
K: Prof Tanczer's citations in charity and practitioner documents on domestic abuse and the IoT, including: AVA. (2019). *Good Practice Briefing: Technology and Violence Against Women – Helping or Harming?* (pp. 1–9) [Supplied] & practitioner's 'statements' [Available on request].