Full bibliographic citation:

Shere ARK, Nurse JRC and Flechais I (2020) 'Security should be there by default': Investigating how journalists perceive and respond to risks from the Internet of Things. In*: 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 1 September 2020, pp. 240–249. IEEE Computer Society. DOI: 10.1109/EuroSPW51379.2020.00039.

Available at:

https://eusec20.cs.uchicago.edu/eusec20-Shere.pdf

https://www.computer.org/csdl/proceedings-article/euros&pw/2020/859700a240/1o8qn16VCda

Abstract:

Journalists have long been the targets of both physical and cyber-attacks from well-resourced adversaries. Internet of Things (IoT) devices are arguably a new avenue of threat towards journalists through both targeted and generalised cyber-physical exploitation. This study comprises three parts: First, we interviewed 11 journalists and surveyed 5 further journalists, to determine the extent to which journalists perceive threats through the IoT, particularly via consumer IoT devices. Second, we surveyed 34 cyber security experts to establish if and how lay-people can combat IoT threats. Third, we compared these findings to assess journalists' knowledge of threats, and whether their protective mechanisms would be effective against experts' depictions and predictions of IoT threats. Our results indicate that journalists generally are unaware of IoT-related risks and are not adequately protecting themselves; this considers cases where they possess IoT devices, or where they enter IoT-enabled environments (e.g., at work or home). Expert recommendations spanned both immediate and longterm mitigation methods, including practical actions that are technical and socio-political in nature. However, all proposed individual mitigation methods are likely to be short-term solutions, with 26 of 34 (76.5%) of cyber security experts responding that within the next five years it will not be possible for the public to opt-out of interaction with the IoT.