Extended Abstract for CADE 2021

How Not To Be Seen: Privacy and Security Considerations in the Design of Everyday Wearable Technology

Helen Oliver*[1,3] and Richard Mortier[2]

[1, 2] Department of Computer Science and Technology, University of Cambridge, UK.
(E-mail: helen.oliver@cst.cam.ac.uk, richard.mortier@cst.cam.ac.uk)
[4] The Alan Turing Institute, UK

Aim and Scope of the Study

From 2017 to 2020, we conducted a research through design to address a number of identified obstacles to adoption of wearable computing. One obstacle was a perceived failure to design wearables for emotional engagement [1] [2] [3]. To address this, we began the inspiration phase with a participatory design process with an open-ended brief, instead of the typical approach of starting with a design exemplar. In this way, we elicited concepts from the participants to discover what kinds of everyday wearables they desired [4], rather than their preferences for some particular device type like an activity monitor [5]. The obstacles interrelate, and the outcome of our investigations against the obstacle of poor emotional engagement, give cause to reflect on another of the obstacles: **privacy.** This paper will reflect on the privacy issues evoked by our experience.

Materials and Methods

The study is described in [4]. The only limit imposed on the participants was that the devices must be everyday connected wearables: i.e. for use in routine rather than specialist (e.g. medical) situations, and capable of transmitting or receiving data. Adult participants were recruited from the general public through workshops at a makerspace. At a series of workshops, each of eight participants told a story in the form of a design fiction, and iterated their fictions until finalized. The fictions described the most desirable form of everyday wearable each participant could imagine. The (by then six) participants voted for the fiction that best expressed their desires for a real-world wearable; which, after a user-centred design process involving text analysis and 1-1 interviews, became a technology probe in the form of the Gallery Necklace. This was a statement necklace featuring an Adafruit eInk breakout board on a Feather M0 Wifi, and dynamically displayed the wearer's artwork. The participants wore their necklaces in-the-wild and sent feedback throughout 2019, before revisiting their design fictions in early 2020, in an attempt at speculative mediation analysis [6].

Our software infrastructure provided for privacy of personal data by using Dataswift's Hub-of-all-Things (HAT) personal data account as an endpoint. The HAT sends and receives data (for the technology probe, a “Hello World) using HTTPS, and stores it in an individual database to which the individual user owns the rights. However, the transmission and storage of data was not the only privacy issue to be dealt with in the process of designing and building even the most minimally functioning wearable technology probe.

Discussion and Findings

The purpose of the Gallery Necklace – even if styled very plainly – was **display.** It existed to be seen, to externalize the wearer’s personality into the artwork on the screen, to hook others into conversation with the wearer through its changing images and unusual casing. This alterity relation to the wearer [7] is the **opposite** of the aesthetic and function of mainstream wearable technology.

Yet, this is what our participants asked us to make for them, given that they could have anything [that was an everyday connected wearable, that we could make in the real world].

In talking about wearable technology and privacy, the aspect most often discussed is the privacy of the personal data processed by the body-worn device. However, consumer wearables usually strive for as bland an appearance as possible, and hearables (ear-worn devices) may be invisible in use.

Why do mainstream wearables try not to be seen, or at least not to draw attention to themselves? Unlike Ihde's [7] example of perfectly/pointlessly invisible clothing, connected earbuds function in an embodiment relation through which the wearer gets the smartphone to make calls or play music; so they only need to be visible enough to pick up, don and doff. This is consistent with Ihde's view of clothing as borderline with embodiment relations, experienced in the background. One effect of backgrounding wearables through bland appearance is *versatility:* the device will coordinate with most outfits, which is especially important for (costly) continuously-worn devices like smartwatches and fitness monitors. These wrist-worn devices are the most popular consumer wearables, typically having a hermeneutic relation to the wearer, who can use them to view their own biodata [7].

Another factor is the *nondisruptiveness* of the device functionality; for example, the earliest function of a smartwatch was to show notifications from the smartphone in situations where handling a phone would be inappropriate. Jacob and Dumas [8] considered the privacy aspects of wearables using a hug-from-a-distance device for couples. Making sure the remote hug message was only detectable to the couple, and not to bystanders, was important not only for nondisruptiveness and social acceptability, but to preserve the intimacy and thus the emotional quality of the communication.

The case of Jacob and Dumas' hug-from-a-distance shows how close nondisruptiveness is to privacy of the wearer from bystanders. Anderson's [9] explanation of the term *privacy* is apposite here: my privacy is breached "If my neighbour cuts down some ivy at our common fence with the result that his kids can look into my garden and tease my dogs". Anderson goes on to define privacy as "the ability and/or right to protect your personal information and extends to the ability and/or right to prevent invasions of your personal space". Body-worn devices are inherently bound to the wearer's personal space. How might the privacy of a hug-from-a-distance system be threatened? By leakage of the personal data from the device or from an app; by an attacker sending hugs as a man-in-the-middle to the unsuspecting partner; by the hug system's presence or usage being exposed to bystanders, either through network activity (most wearable devices use Bluetooth, which is not very secure) [10] or by **attention's being drawn to its physical presence.** The author of the design fiction that inspired the Gallery Necklace was the only male in the group; we gave his necklace a minimalist style in keeping with the style of his paper prototypes, but also to avert the risk of hostile reactions from other men.

What about wearable devices which (unlike the Gallery Necklace) have monetary, rather than just sentimental value? Smartwatches are paired with mobile phones, which are a desirable "stealable," snatchable item. According to the UK's Office for National Statistics[1], the individual risk seems low, but awareness of that risk is necessary in public. Loss of personal data, which can be wiped remotely, is less of a problem than loss of the handset.

A smartwatch is harder to steal from the wearer's wrist than a phone from the hand; but a smartwatch is expensive and visible. The impulse driving the project was my own personal desire to

[1]https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/focusonpropertycrimeappendixtables

develop an everyday connected wearable that I would want to wear; and the safety of wearing it in public is part of that. Women are taught to carry their handbag in front of them, like an American football, to visibly protect it from thieves and to make it easy to let go if someone does try to steal it. We are warned against slinging a bag across the body, because the strap can be used as a handle to pull the victim to the ground. Against this background of prior acculturation, I personally would have concerns at the back of my mind about the damage that could be done if someone tried to pull a watch – which would be the most expensive watch I had ever owned - off the only left wrist I have ever owned.

Smart NFC (near field communication) payment rings obviate the need to pull out a wallet or ticket, they do not need a power supply, and a payment limit can be set[2]. Some add functionality to open doors, and the option for automatic top-up of funds; so an adversary has a motive to follow the wearer home. A hallway check of security researchers from various countries elicited a mix of objectivist [11] hacking tips, and a spectrum of anecdotal opinions about the relative risks to fingers, hands, bags, and apartment contents in Russia, Malaysia, Mexico or Scotland. How comparatively safe the ring *feels* depends on the context. How much is the inescapability of existential risk [11] and how much is a privacy hole in my bucket of obstacles to wearable computing?

Conclusions

Although the Gallery Necklace as implemented was not a "stealable" piece of jewellery with any appearance of commercial value, there were still security considerations that needed to be addressed in the implementation, not only of the software but of the device's appearance as a statement necklace that was built to draw attention and comment.

In this presentation I will discuss the challenges of designing everyday wearable technology for privacy and security, using the experience of hand-crafting the Gallery Necklace as a motivating example.

REFERENCES

[1] Wallace, J.: 'Emotionally charged: a practice-centred enquiry of digital jewellery and personal emotional significance', Doctor of Philosophy, Sheffield Hallam, 2007.
[2] Maciocci, G.: 'Me too wearables', *Medium*, 11 December 2013. https://medium.com/@augmentl/me-too-wearables-2a035202e9fe. Accessed 6 May 2021.
[3] Hunn, N.: 'The market for smart wearable technology: a consumer centric approach', WiFore Consulting, February 2015. http://www.nickhunn.com/wp-content/uploads/downloads/2014/08/The-Market-for-Smart-Wearables.pdf. Accessed 6 May 2021.
[4] Oliver, H.: 'Design fiction for real-world connected wearables', In *The 5th ACM Workshop on Wearable Systems and Applications - WearSys '19*, 59–64. Seoul, Republic of Korea: ACM Press, 2019. https://doi.org/10.1145/3325424.3329664.
[5] Pateman, M., Harrison, D., Marshall, P., and Cecchinato, M. E.: 'The role of aesthetics and design: wearables in situ', In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18*, 1–6. Montreal QC, Canada: ACM Press, 2018. https://doi.org/10.1145/3170427.3188556.
[6] Verbeek, P-P: 'Technology design as experimental ethics', In S. van den Burg and Tsj. Swierstra, *Ethics on the Laboratory Floor*. Basingstoke: Palgrave Macmillan, pp. 83-100. ISBN 9781137002921
[7] Ihde, D.: 'Technology and the Lifeworld: From Garden to Earth', Chapter 5. Indiana University

[2]https://payspacemagazine.com/tech/smart-rings-with-nfc/

Press, 1990.
[8] Jacob, C., and Dumas, B: 'Designing for intimacy: how fashion design can address privacy issues in wearable computing', In *Proceedings of the 2014 ACM International Symposium on Wearable Computers Adjunct Program - ISWC '14 Adjunct*, pp. 185–92. ISWC '14, 13-17 September 2014, Seattle. ACM Press, 2014. DOI: https://doi.org/10.1145/2641248.2641353.
[9] Anderson, R.: 'Security engineering: a guide to building dependable distributed systems', Hoboken: John Wiley & Sons, 2020.
[10] Bada, M.: A cybersecurity guide to using fitness devices. In press, 2021.
[11] Coeckelbergh, M.: '*Human Being @ Risk'*, Vol. 12, Chapter 3. Philosophy of Engineering and Technology. Dordrecht: Springer Netherlands, 2013. https://doi.org/10.1007/978-94-007-6025-7.