UNIVERSITY OF OXFORD

DEPARTMENT OF COMPUTER SCIENCE

Beyond the Individual

Exploring Data Protection by Design in Connected Communal Spaces

Martin J Kraemer
Department of Computer Science
University of Oxford

2020 USENIX Conference on
Privacy Engineering Practice and Respect (PEPR ’20)
October 15–16, 2020. Virtual event.

EPSRC
Engineering and Physical Sciences
Research Council

CENTRE FOR
DOCTORAL TRAINING
in CYBER SECURITY

ico.
Information Commissioner's Office
Grant
Recipient

Data Protection and Privacy

- The use of internet-connected technology is often accompanied by concerns of data protection and privacy
- Legislation is traditionally concerned with individuals’ right to privacy (and data protection in the EU); for example …
    - The General Data Protection Regulation (GDPR) has a ‘household exemption’
    - The California Consumer Privacy Act (CCPA) includes ‘households’ as deserving of data protection rights without a clear definition of personal information in relation that concept
- In the academic literature, privacy beyond the individual has been approached in different (technological) contexts providing different interpretations, but there is a lack of understanding privacy in communal spaces.

Problem Space

- Communal and shared spaces such as homes, cafes, or airports are equipped with ambient and pervasive internet-connected technology
- Heterogeneous groupings of individuals with dynamic social structures, (un)attributed responsibilities, and varying levels of skill
- Privacy is context dependent and situational, and there's a lack of understanding privacy beyond the individual

How can research explore and facilitate design for privacy in communal spaces

Research Approach

Participatory Co-Design Workshops

- Inspired by *Future Workshop* format: critiquing the present, envisioning the future, and implementing (not included in workshops)
- Focus on *social and communal factors* of technology use inherent to the method
- Facilitate workshops using design techniques and artefacts

Part A – critiquing the present

(1) **Exploring** – social and physical aspects of shared spaces
through affinity diagramming and sketching (similar to *context scenarios*); we chose 'home' and 'café'

(2) **Attuning** – to popular data protection issues,
e.g. browser bar padlocks and mobile application permissions (researcher led)

(3) **Reflecting** – on further issues of data protection
facilitated by guiding questions (participant led)

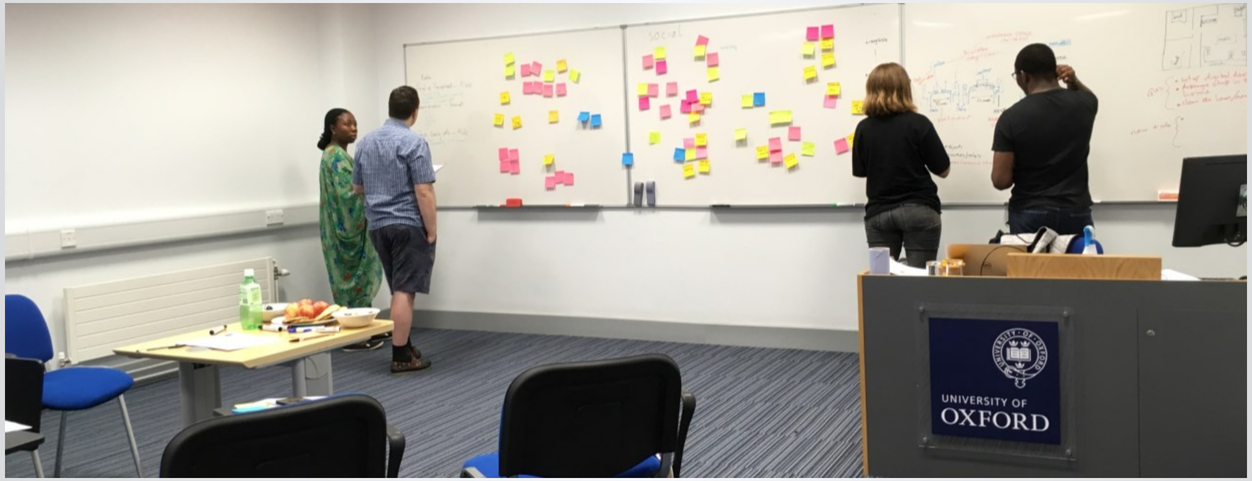
Part B – Envisioning the future

(1) **Designing** – for either shared space from Part A.
assist when prompted; *optionally,* provide a set of personas.

(2) **Re-designing** – for a different shared space from Part A.
Optionally, exchange sketches from Part A between groups

(3) **Reflecting** – on design process and presenting solution

Piloting the Approach

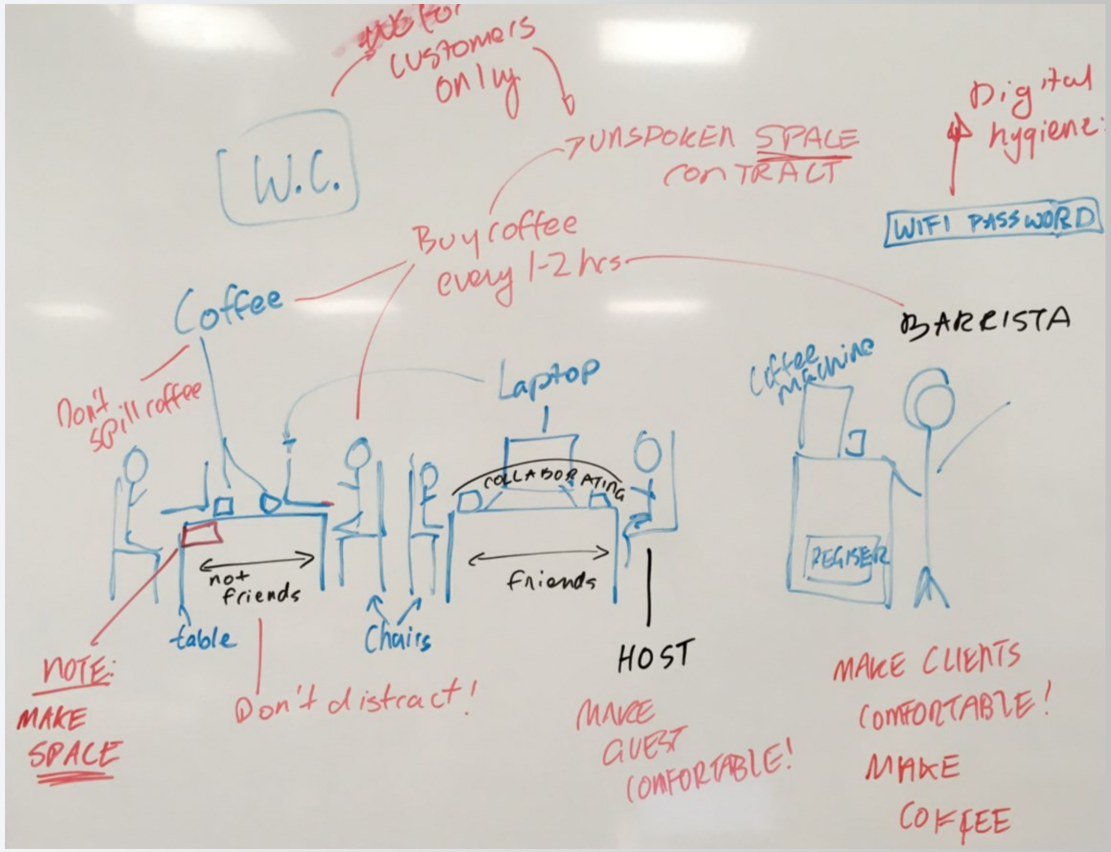


Four groups of students and expert researchers **co-designed a ‘good’ internet connection experience** considering usable security and privacy for homes and cafes

The ‘Data Flush’

by Group 2

- Focus on achieving anonymity on the WiFi network during and after use
- Devices remembered for 24h, and network not remembering device seen as proof of erasure
- Design idea: ***data flush*** – provides reassurance of data deletion by tapping out
- Initially only considered friends sharing a table; last person to leave flushes data at table
- Café Context 1 included strangers sharing a table; considering, the group moved the button from the table to the door

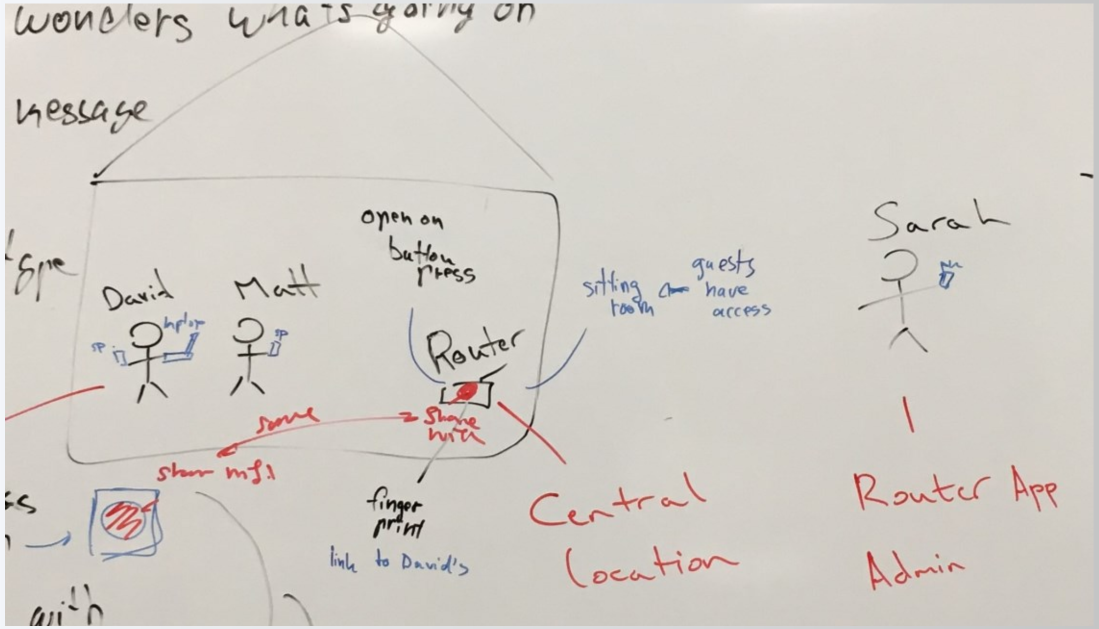


Café context 1: Sketch of a café as seen by Group 1

‘Put the password in the kitchen cupboard’

by Group 4

- Initially technical ‘expert’ counter measures for the router considered
- Considering other personas with varying aptitudes and skills, the proposed solution seemed impractical
- The group considered technical, social, and physical solution alternatives
- For example, a ‘touch and connect’ solution but also placing the password in a kitchen cupboard as a semi public space



Solution sketch 1: secure and accessible network connection setup including connect button, connect app, and notes on the location of the router

Some Reflections

On our methodology

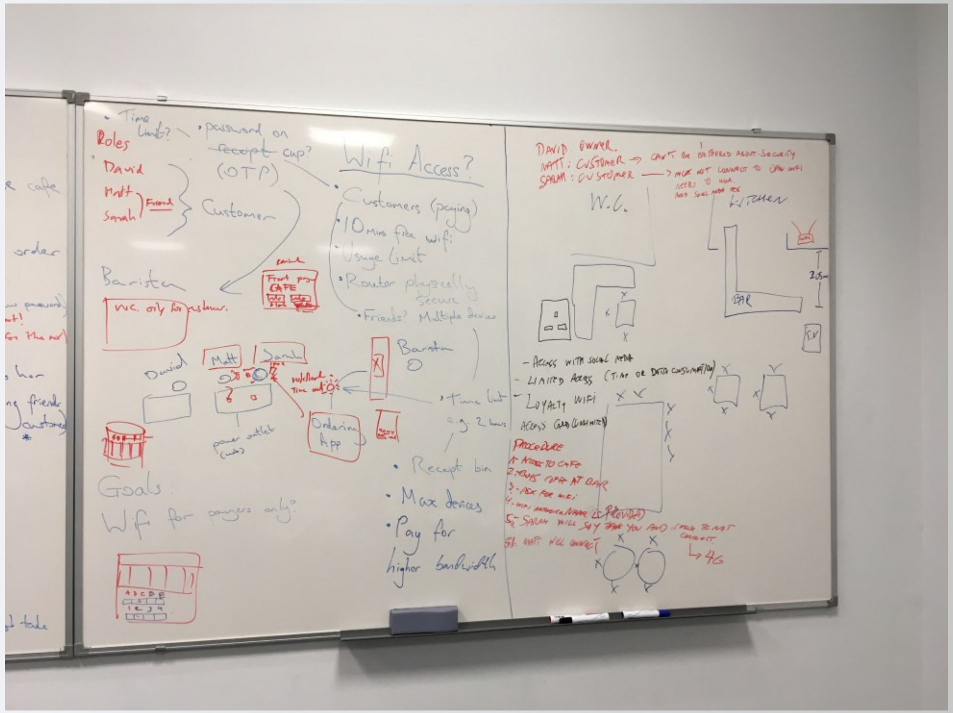
- *limitations*: pilot-groups included students only, somewhat limited in their lived experiences; two very different contexts, the café as more public and the home as private space
- Insights from design artefacts allowed participants readjust the appropriateness of their solutions, e.g. personal characteristics from personas or ‘rules and relationships’ from context sketches
- Artefacts can help surface some of the ‘tacit’ contextual variations that influence co-design for privacy

On our findings

- Potential role of social groups in framing design, e.g. ‘friends’ with common goals can share data protection responsibilities
- Focus on relationships of people in shared spaces, e.g. the need for individuals to considering the abilities of others
- Resourcefulness of participants to enable data protection in communal spaces, e.g. password in the kitchen cupboard as semi-private space

Implications

- Communal spaces and concomitant relationships are important considerations for design of internet-connected technologies
- Structured contextual artefacts capturing social and physical aspects of communal spaces can inform design for data protection
- Communal participatory design approaches can provide innovation for privacy beyond the individual



Questions?

Martin J Kraemer
Doctoral Researcher

martin.kraemer@cs.ox.ac.uk

www.martin-kraemer.net

Acknowledgments
This research is part of our project ‘Informing the Future of Smart Homes: Enabling Data Protection by Design and by Default’ funded by an Information Commissioner’s Office UK research grant.
https://digiwell.web.ox.ac.uk/informing-future-smart-homes

Collaborators on the presented work are Dr Norbert Nthala, Prof. Ivan Flechais, Paula Fiddi, and William Seymour.