IoT Security and Privacy

INFR11158/11230 Usable Security and Privacy

Dr. Jingjie Li

19/03/2024

THE UNIVERSITY *of* EDINBURGH

Overview

- Recap - consent
- IoT
- Take-home


TikTok
helped me grow
my busine
NBC NEWS

Consent

Consent in General Data Protection Regulation

The basic requirements for the effectiveness of a valid legal consent are defined in Article 7 and specified further in recital 32 of the GDPR. **Consent** must be freely given, specific, **informed** and unambiguous. In order to obtain freely given consent, it must be given on a voluntary basis. The element “free” implies a real choice by the data subject….

Right to be informed

There is a need for transparency regarding the gathering and use of data in order to allow EU citizens to exercise their right to the protection of personal data. Therefore, the General Data Protection Regulation (GDPR) gives individuals a **right to be informed** about the collection and use of their personal data, which leads to a variety of information obligations by the controller.

Informed consent in real life and in research

An advertisement should:

- Be short and easy to read or decide to ignore
- Explain the main content of what participants will be asked to do
- Explain what the costs, benefits, and risks of participating are
- State who to contact about the research in case of concern
- State if the research has been through ethical review

A consent form should:

- Who you are
- What the study involves, what they will be asked t do
- What kind of data will be collected and how it will be used
- What rights the participant has
- Compensation, if any

We are students in the Human-Computer Interaction course. For our first coursework we are studying how students at the University of Edinburgh use calendaring systems such as paper calendars, Google Calendar, and Office 365 Calendar.

In this survey we are investigating how people use their online calendars so that we can better understand their calendar-related needs and choices. We will ask you for some information about yourself, about the way in which you use computers and the internet, about the tools you use to manage your timetable and other events.

Completing the survey will take about 10 minutes. You can interrupt the survey at any time and return to finish it later. All the data that you provide will be stored on SurveyMonkey and user-level access will be restricted to our group. Questions marked with a red star are mandatory - you will need to answer them in order to complete the survey. Data you provide will be deleted two months after the last day of this school term.

This project has undergone ethical screening in accordance with the University of Edinburgh School of Informatics ethics process (RT1432).

Do you agree to take part in this study, and do you agree that I can use your data for my HCI student project?

Social media has been a great resource for people to do a wide range research; But people are becoming more and more careful nowadays. What are the ethical considerations in using social media data for research?

School of Informatics Intranet
INFWEB

Using secondary and social media data

Guidance on ethical considerations for using secondary data and data from social media in research projects.

This information is largely adopted from the LEL advice pages in PPLS. You can access the original pages in relevant sections below. Please contact the Informatics ethics committee (inf-ethics@inf.ed.ac.uk) with any questions about the use of secondary data and/or social media data in Informatics research.

Note that for both secondary data and social media data, **the use of data is not automatically ethical just because it is legally accessible.** Always consider your research question and the participants from whom data is collected; for instance if the research is conduct on a group considered vulnerable (e.g. a forum on mental health) the ethical considerations are much more complex than research conducted on less vulnerable groups (e.g. football fans).

Secondary data - ethics application may be required

Secondary data is sometimes available through established corpora. If you are using data from an existing corpus, there is typically no need to apply for further ethical approval, **however** you should continue to treat any data from human participants in an ethical manner. Considerations include:

- If the data are in the public domain, you must abide by any requirements stated by the corpus provider, including with respect to anonymity, or any other conditions on use.
- Some corpora may require ethical approval, especially corpora that include physical or mental health data, or corpora that contain data that could be used de-anonymise individuals (e.g. when free-text responses are allowed).

Some ethical practices

- Follow the terms of use
- Obtain informed consent when possible
- Check our ethics guidelines for more! https://resource.ppls.ed.ac.uk/lelethics/index.php/frequently-asked-questions/research-with-social-media-data/

Case studies in Ethics and Security

EXPERIMENTAL EVIDENCE OF MASSIVE-SCALE EMOTIONAL CONTAGION THROUGH SOCIAL NETWORKS

by Adam D. I. Kramer, Jamie E. Guillory, and Jeffrey T. Hancock

Aka Facebook emotion contagion study

“We show, via a massive (*N* = 689,003) experiment on Facebook, that emotional states can be transferred to others via emotional contagion, leading people to experience the same emotions without their awareness. We provide experimental evidence that emotional contagion occurs without direct interaction between people (exposure to a friend expressing an emotion is sufficient), and in the complete absence of nonverbal cues.”

http://www.pnas.org/content/111/24/8788.full

The study

- All Facebook users who spoke English qualified
- Two groups: positive and negative emotions
- Positive/negative posts where then suppressed from the news feed
- 689,003 participants randomly selected by user id
- Saw an impact
  - When positive posts withheld the participant’s posts got more negative
  - When negative posts withheld the participants posts got more positive
  - Withdrawal effect: people who saw less emotion posts less likely to express themselves for several days

Think-pair-share

- Does the Facebook Emotion Contagion study fit the requirements of the Belmont Report?

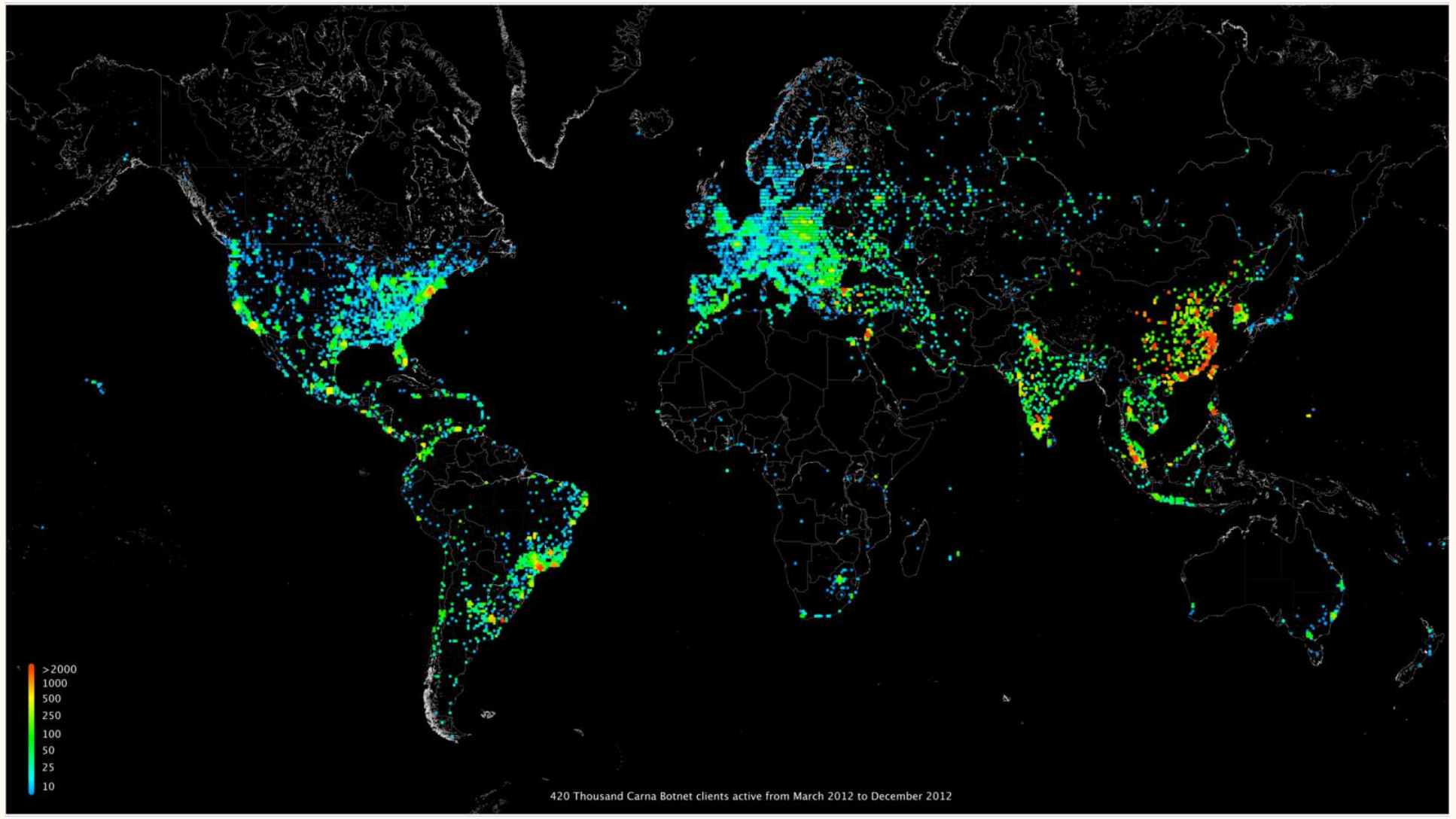
The Belmont Report (1974)

- Respect for persons
  - protecting the autonomy of all people and treating them with courtesy and respect and allowing for informed consent. Researchers must be truthful and conduct no deception
- Beneficence
  - The philosophy of "Do no harm" while maximizing benefits for the research project and minimizing risks to the research subjects
- Justice
  - ensuring reasonable, non-exploitative, and well-considered procedures are administered fairly – the fair distribution of costs and benefits to *potential* research participants – and equally.

http://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/index.html

Mapping the Internet: Someone made the most detailed map of the internet ever by hacking into just under half a million computers

http://motherboard.vice.com/blog/this-is-most-detailed-picture-internet-ever


>2000
1000
500
250
100
50
25
10
420 Thousand Carna Botnet clients active from March 2012 to December 2012

Is it ethical to use this data to do good things?

THE EMPEROR'S NEW SECURITY INDICATORS: AN EVALUATION OF WEBSITE AUTHENTICATION AND THE EFFECT OF ROLE PLAYING ON USABILITY STUDIES

Stuart E. Schechter, Rachna Dhamija, Andy Ozment, and Ian Fischer

http://www.usablesecurity.org//emperor/emperor.pdf

Will bank customers enter their passwords even if their browsers' [security UI element] is missing?

Study design

- Participants recruited using on-campus flyers
- Flyers said the participant could “earn $25 and make online baking better”
- No mention of security or privacy in any advertising materials or consent form (deception study)
- Participants came to the lab and used a lab computer
- Computer was pre-setup to attack the connection between the bank and the user

To handle ethics the researchers:

- Notified participants that their actions would be recorded
- System did not record passcodes or other private data
- Care was taken with the technical design to make sure the participant’s bank credentials remained safe
- Participant was debriefed after the study
- Participant was told how to protect themselves in the future

BROWN UNIVERSITY P2P

Andy Pavlo

https://hardware.slashdot.org/story/09/04/13/0120226/grad-student-project-uses-wikis-to-stash-data-miffs-admins

"Two graduate students at the Ivy League's Brown University built a P2P system to use abandoned wiki sites to store data. The students were stealing bandwidth from open MediaWiki sites to send data between users as an alternative to BitTorrent. There was immediate backlash as site operators quickly complained to the University. The project appears to be shutdown, but many of the pages still remain on the web. The project homepage was also taken down and the students posted an apology this afternoon."

https://hardware.slashdot.org/story/09/04/13/0120226/grad-student-project-uses-wikis-to-stash-data-miffs-admins

Internet of Things


Hello
Barbie
HELLO
HELLO
HELLO
PRESS BELT
& TALK
WARNING:
6+
belkin
NETCAM
ANNKE
HD 720P Video Monitoring
Sparkle I
ANNKE
netatmo
The Weather Station for Smartphone
La Station Météo pour Smartphone
ring
VIDEO
DOORBELL
Try me!
SEE & SPEAK WITH VISITORS
MOTION DETECTION
WI-FI CONNECTED
fitbit
Balance Wi-Fi intelligente
Báscula inteligente Wi-Fi
PIXSTAR
FotoConnect XB
Wi-Fi 10.4"
Instantly receive photos from those you love
from anywhere in the world
RATIO 4/3
Email

Introducing

echo studio

"Alexa, play the Best of 3D Musi

Press the mic off button to disconnect the microphones

“Internet of Things”

- Previously known as:
  - Ubiquitous computing
  - Ambient computing
- Idea is that the computers are embedded into the world around people, effectively pushing computation into the surrounding infrastructure, rather than in devices we carry around.
- Large issues:
  - Privacy
  - Security
  - Trust
  - Battery
  - Computational power

I wanted to buy [household appliance] and I found a really great one that was highly rated and had [a feature I really wanted].

Then I discovered that it was internet enabled. So I went and found a different "dumb" one and bought that because it was safer.

Users are loosing trust in the safety and privacy of the IoT and this is a big problem… partially because they are correct.

Hotel ransomed by hackers as guests locked out of rooms

The Local
news.austria@thelocal.com

28 January 2017
10:42 CET+01:00

crime

Share this article

Photo: CEN

One of Europe's top hotels has admitted they had to pay thousands in Bitcoin ransom to cybercriminals who managed to hack their electronic key system, locking hundreds of guests out of their rooms until the money was paid. (Updated)

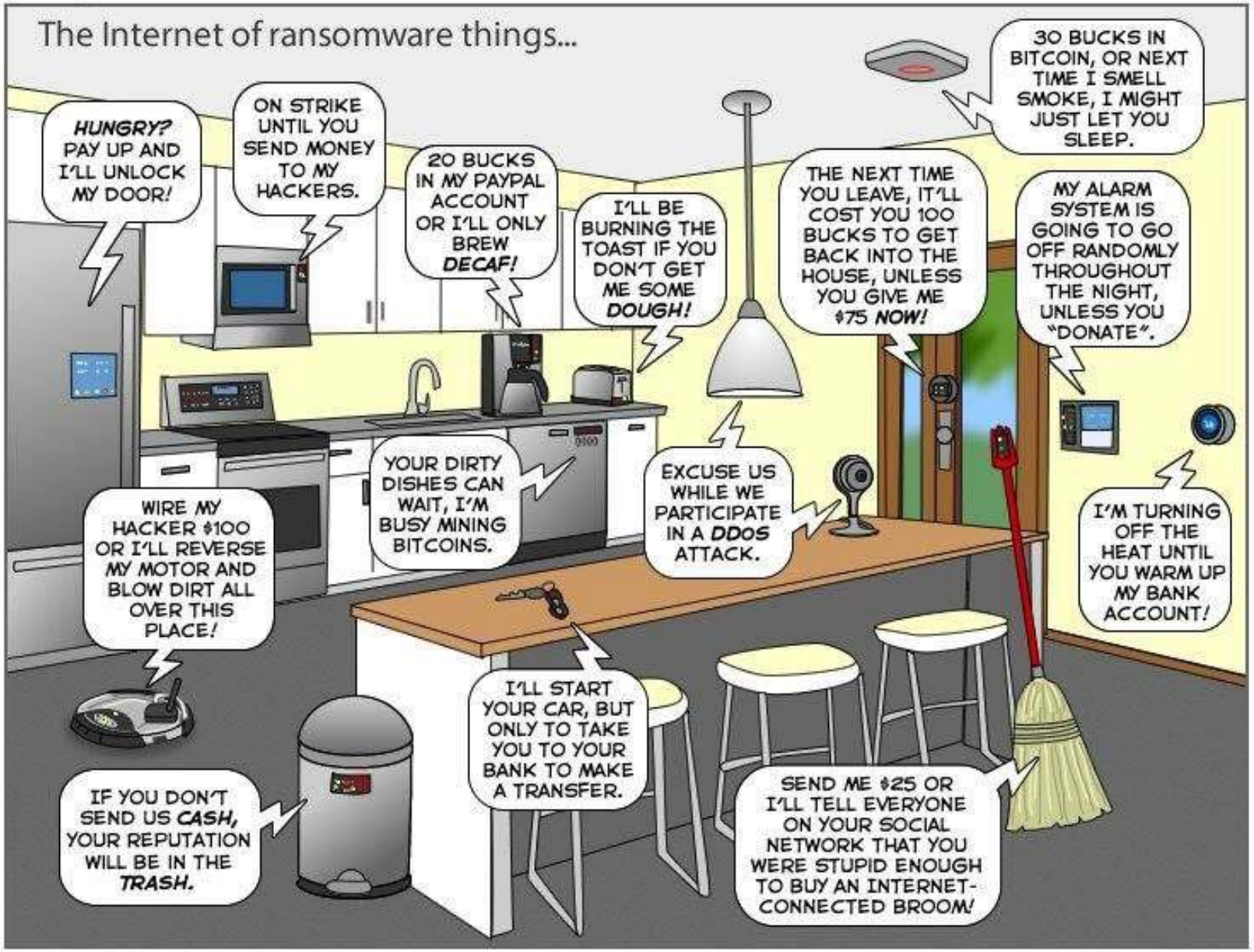
Furious hotel managers at the Romantik Seehotel Jaegerwirt, a luxurious 4-star hotel with a beautiful lakeside setting on the Alpine Turracher Hoehe Pass in Austria, said they decided to go public with what happened to warn others of the dangers of cybercrime.

Ring's smart doorbell can leave your house vulnerable to hacks

The $199 Ring Video Doorbell may be "smarter" than your average buzzer, but a major vulnerability can leave your Wi-Fi network wide open to hackers.

Megan Wollerton January 13, 2016 11:50 AM PST

The Joy of Tech™ by Nitrozac & Snaggy



joyoftech.com

Why don’t people protect themselves?

1. People are not **aware** of the risks or protection mechanisms.

2. People cannot **use** the available protection mechanisms.

3. People do not **care** about security and privacy.

Lemon markets

Security and privacy in IoT is currently a lemon market.

People with purchasing power cannot differentiate between a “good” device and a “bad” one

What about this iKettle? Is it “safe”? What about “private”?

Larger concern is that you can’t tell from looking at it.

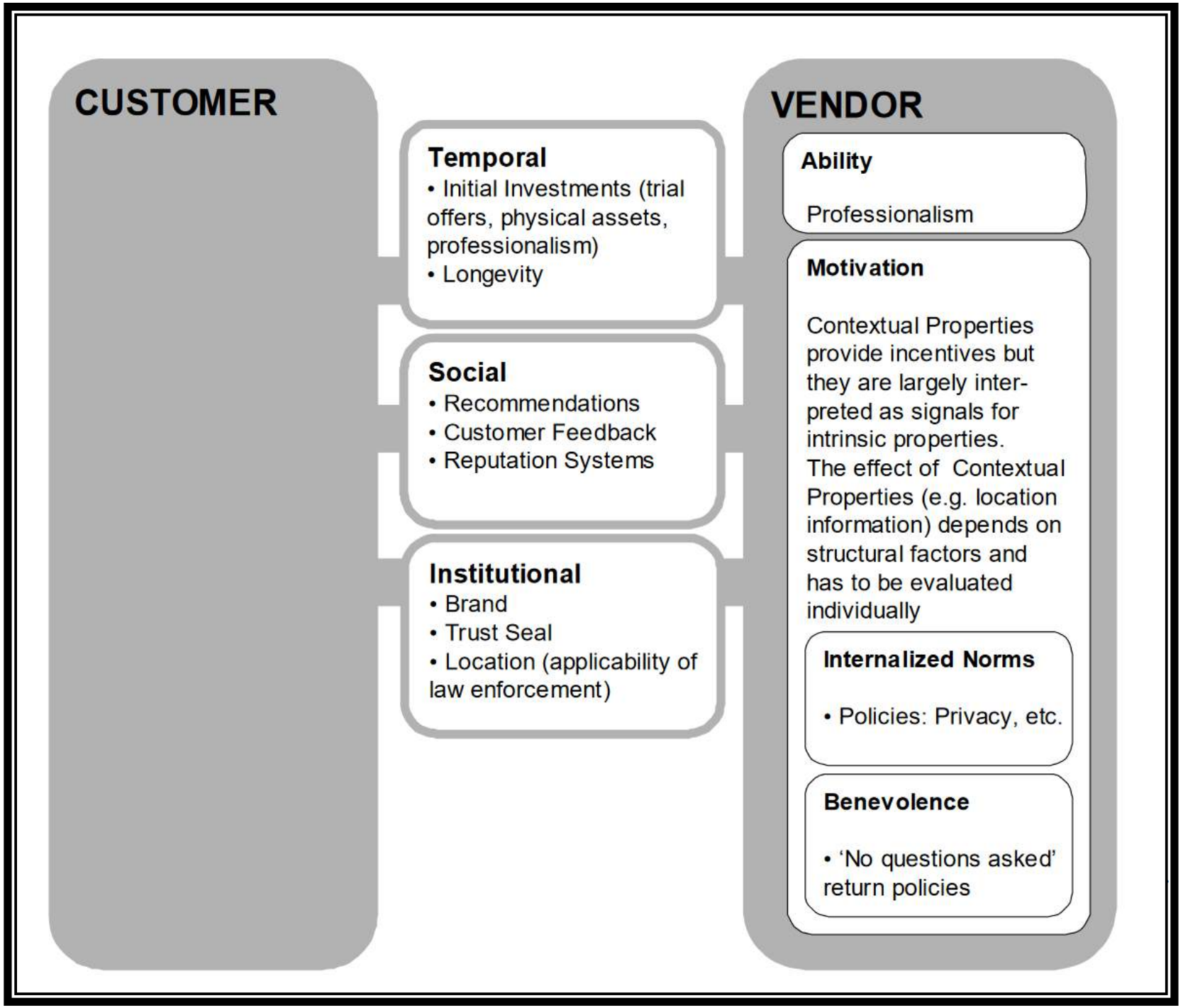
Manuscript: Trust in Mediated Interactions
Oxford Handbook of Internet Psychology

Jens Riegelsberger, M. Angela Sasse, John D. McCarthy

Department of Computer Science
University College London

ABSTRACT

With an increasing number of technologies supporting interaction at a distance, trust in mediated interactions has become a key interest in the field of human computer interaction (HCI). Research covers the role of trust in mediated interactions with other individuals (e.g. in virtual teams) and organisations (e.g. via e-commerce web sites). This chapter synthesises current research into a framework that introduces the key factors that affect trust and trustworthy behaviour. These are *contextual properties* (motivation based on *temporal*, *social*, and *institutional embeddedness*), and the *actor's intrinsic properties* (*ability*, and motivation based on *internalized norms* and *benevolence*). Knowledge of these underlying factors can help designers in structuring the design space and researchers in planning and generalising from studies on trust in mediated interactions.


CUSTOMER
Temporal
• Initial Investments (trial offers, physical assets, professionalism)
• Longevity
Social
• Recommendations
• Customer Feedback
• Reputation Systems
Institutional
• Brand
• Trust Seal
• Location (applicability of law enforcement)
VENDOR
Ability
Professionalism
Motivation
Contextual Properties provide incentives but they are largely inter-preted as signals for intrinsic properties.
The effect of Contextual Properties (e.g. location information) depends on structural factors and has to be evaluated individually
Internalized Norms
• Policies: Privacy, etc.
Benevolence
• 'No questions asked' return policies

How fast can you decide that these items are “good” purchases?

Capturing the Connections: Unboxing Internet of Things Devices

Kami Vaniea
School of Informatics
Informatics Forum 5.23
10 Crichton Street
University of Edinburgh

Ella Tallyn
Design Informatics
78 West Port, Edinburgh
University of Edinburgh

Chris Speed
Design Informatics
78 West Port, Edinburgh
University of Edinburgh

Abstract
Based upon a study of how to capture data from Internet of Things (IoT) devices, this paper explores the challenges for data centric design ethnography. Often purchased to perform specific tasks, IoT devices exist in a complex ecosystem. This paper describes a study that used a variety of methods to capture the interactions an IoT device engaged in when it was first setup. The complexity of the study that is explored through the annotated documentation across video and router activity, presents the ethnographic challenges that designers face in an age of connected things.

Introduction
This pictorial presents an ethnographic method used to study the behaviours of an Internet of Things device during its initial setup and use. The work represents an ethnographic approach to a common computer security practice of observing IoT devices as they are unboxed and begin interacting with the world around them. The

Ring's smart doorbell can leave your house vulnerable to hacks

The $199 Ring Video Doorbell may be "smarter" than your average buzzer, but a major vulnerability can leave your Wi-Fi network wide open to hackers.

Megan Wollerton January 13, 2016 11:50 AM PST

R

Temporal
- Initial Investments (trial offers, physical assets, professionalism)
- Longevity

Social
- Recommendations
- Customer Feedback
- Reputation Systems

Institutional
- Brand
- Trust Seal
- Location (applicability of law enforcement)

VENDOR

Ability

Professionalism

Motivation

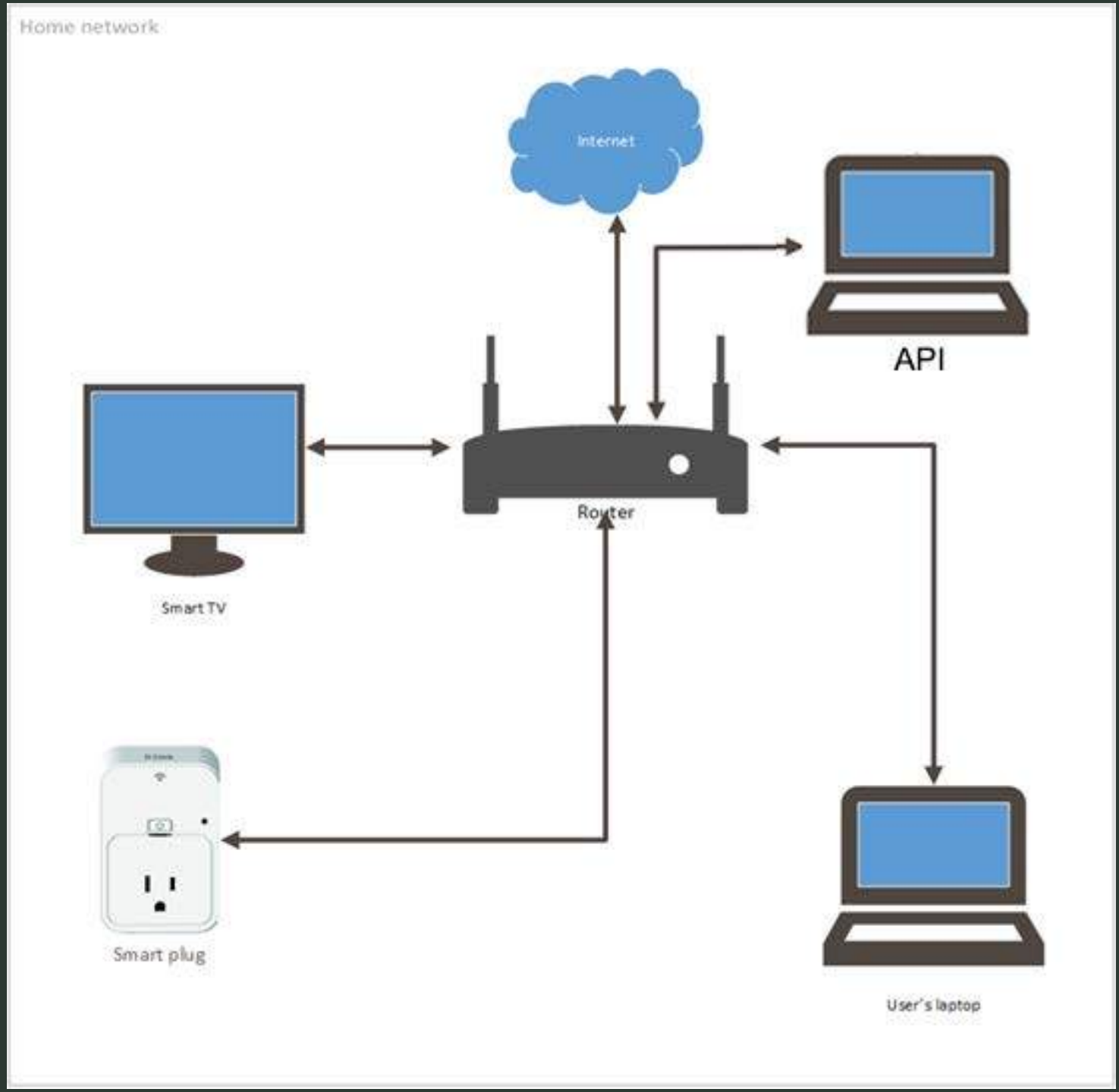
Contextual Properties provide incentives but they are largely inter-preted as signals for intrinsic properties.
The effect of Contextual Properties (e.g. location information) depends on structural factors and has to be evaluated individually

Internalized Norms

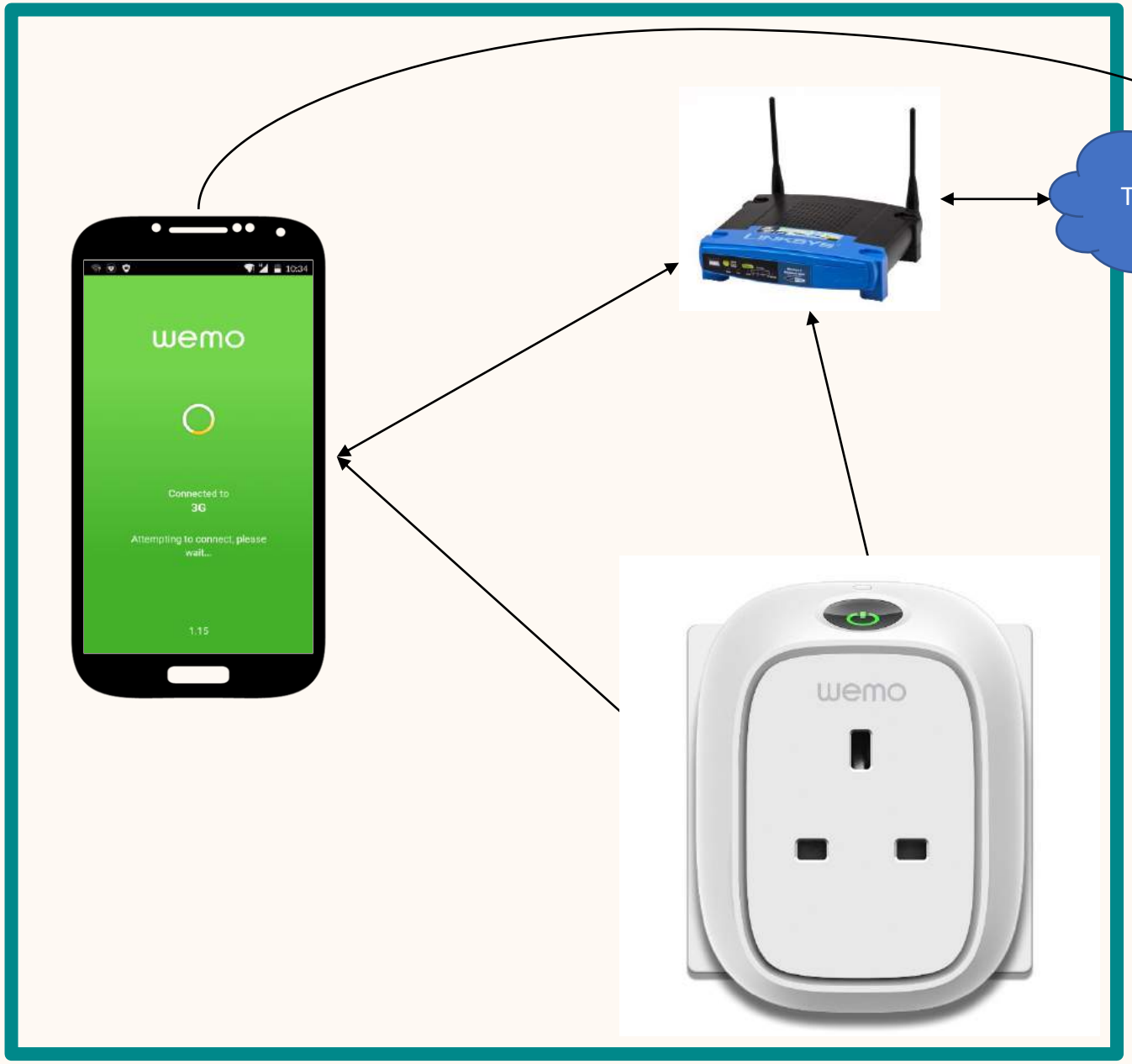
- Policies: Privacy, etc.

Benevolence

- 'No questions asked' return policies


Home network
Internet
API
Router
Smart TV
Smart plug
User´s laptop


The Internet
wemo
Connected to
3G
Attempting to connect, please wait...
1.15
belkin
Belkin
Other Servers


wemo
Connected to
3G
Attempting to connect, please wait...
1.15
The Internet
wemo
wemo
Belkin
Other Servers


2

IoT Network Visualisation - Mozilla Firefox

IoT Network Visualisation

127.0.0.1:5000/#

Search

IoT Network Visualisation

File Live

Live

Window Size: 10

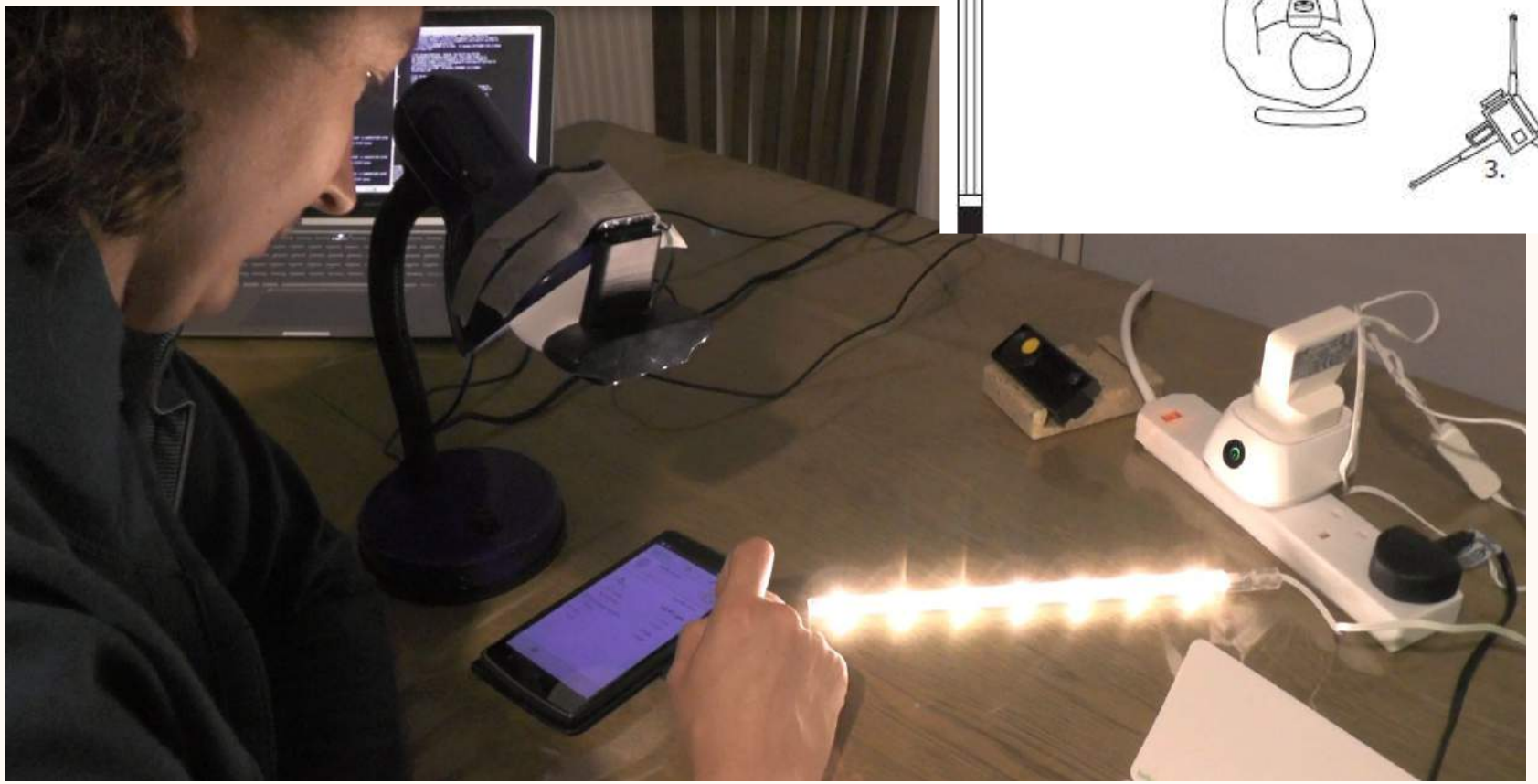
Update Interval: 2

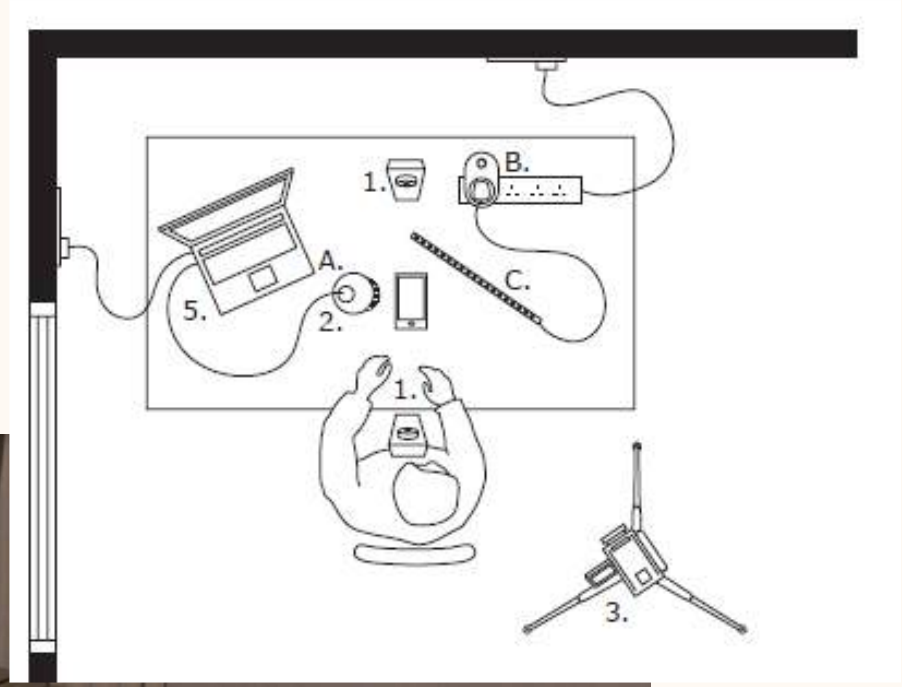
Show Connections

Chart

Devices:

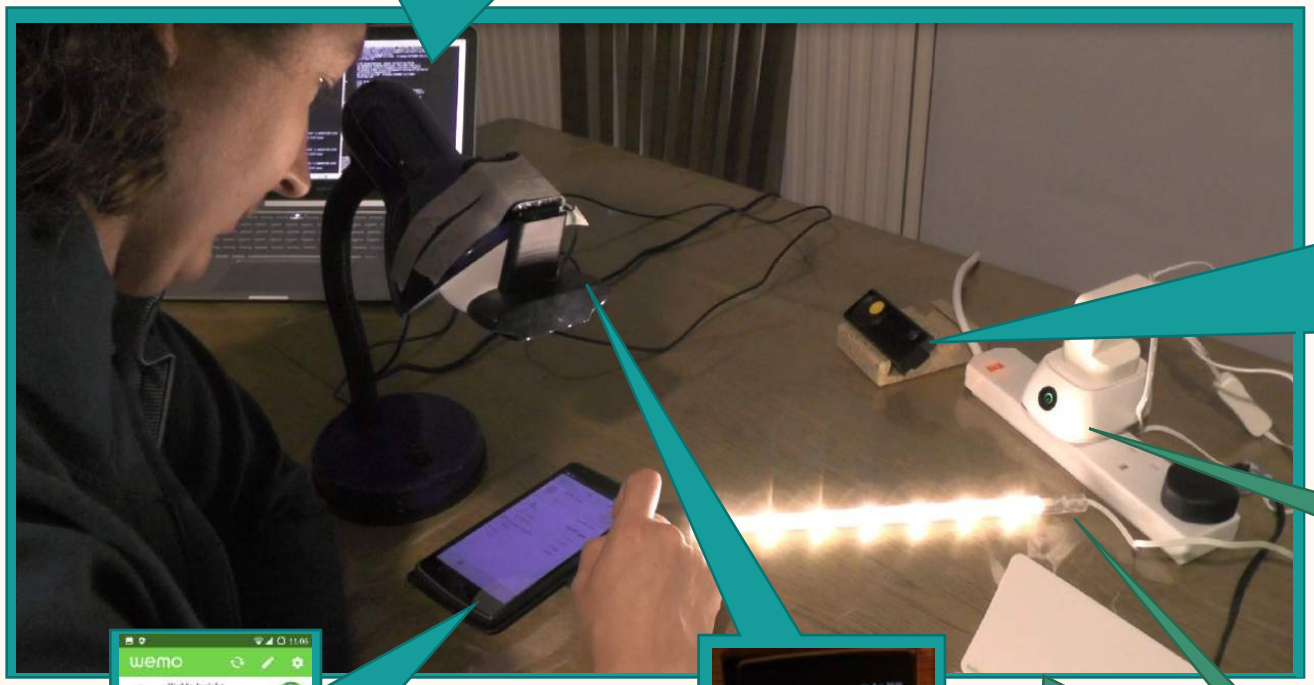
- lenovo-laptop
- MotoG
- Sasmsung-phone
- DragonTouch

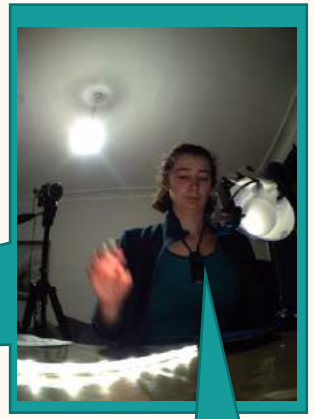



1.
B.
A.
C.
5.
2.
1.
3.

Laptop used to control and monitor status of recordings including the live video from camera positioned over the phone (top left), traffic visible to the router (right) and list of devices connected to the router (bottom left).

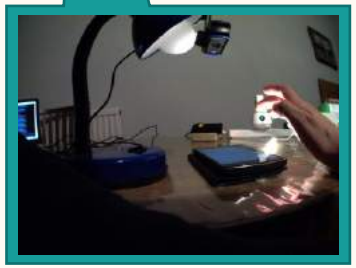
Router (located in another room) captures all network communications between devices and between devices and the internet. Pictured communication is the phone app asking the switch to turn on (red) and the switch reporting that it has turned on (blue).



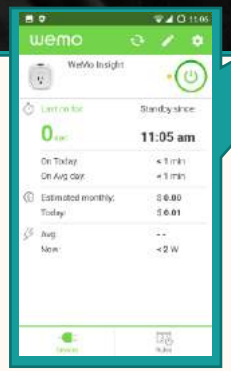


Autographer near the “thing” records the thing’s perspective visually and provides another view of the researcher.

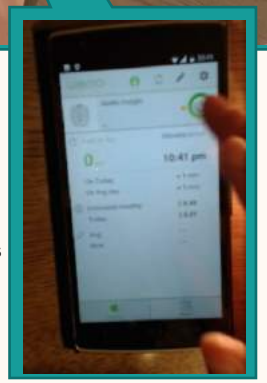
WeMo switch



Phone records continuous screen capture for high-resolution view



Same thing seen two ways



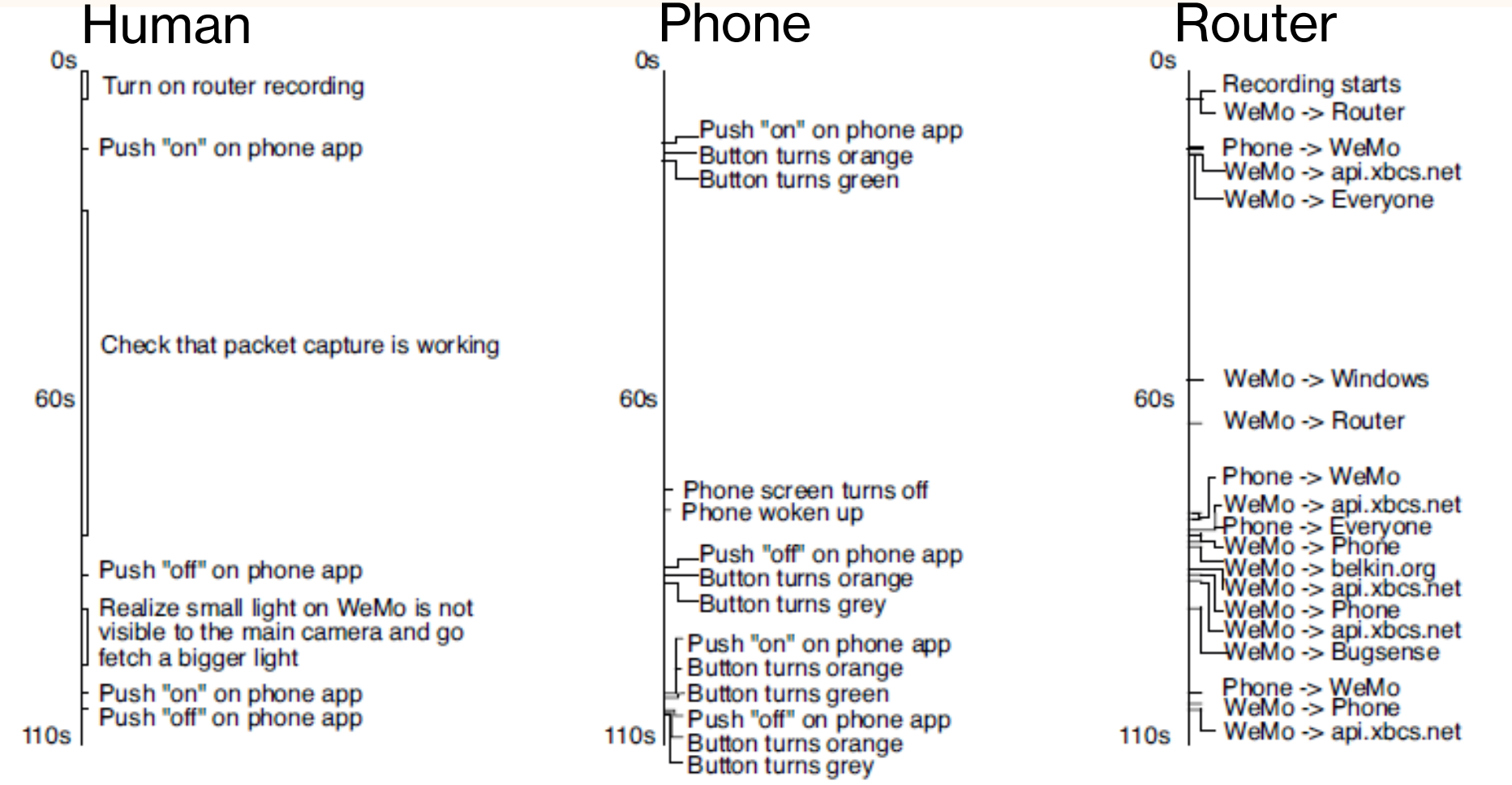
Camera taped to lamp records user’s interactions wit the screen including hovering over buttons and any images that might be blocked from screen capture by phone security software

Setup instructions that came with WeMo

Light showing if WeMo switch is on or off

Autographer around researcher’s neck records their perspective and any out-of-camera events like needing to reset the router.

Human, phone, and router perspectives



Router Yes

Phone Turn on please

Got it Wemo

I'm on now Wemo

Let's start an encrypted chat Wemo

api.xbcs.net Sure

akdfjw;eifjwe;ij Wemo

api.xbcs.net dslkfs;ldkfjs

Anyone have a plug and play service they are sharing? Wemo

I hear you are sharing some services Wemo

Windows Yep, here is a full list ....

You there? Wemo

Router Yes

Phone can you send me the setup data file?

Sure, here you go Wemo

Phone can you send me your current status?

Sure, here you go Wemo

Phone Can you send me your power settings for this home?

Sure, here you go Wemo

Phone Can you send data you have collected so far?

Sure, here you go Wemo

Phone What time do you think it is right now?

Sun, 29 May 2016 224035 GMT Wemo

Phone If any events happen to you in the future please tell me about them.

OK Wemo

Phone If you want to update please tell me that too.

OK Wemo

Phone Just making sure you know I am allowed to turn you on and off.

Understood, here are all the secret codes Wemo

Let's start an encrypted chat Wemo

api.xbcs.net Sure

fewkfbjek>?33 Wemo

api.xbcs.net oerle,,ewjd

Phone Anyone support Belkin protocols?

Remember how you told me to tell you about any events? Some data about my plugins just changed. Wemo

Phone OK

Oh, my home and device ID codes just changed too. Wemo

Phone OK

I've got a problem, I'm behind a home network router so if the phone I have been talking to leaves home I won't be able to talk to it anymore. Could you act as a mediary and connect us if that happens? Wemo

Belkin Sure

Let's start an encrypted chat Wemo

api.xbcs.net Sure

duorllwgar>?d Wemo

api.xbcs.net []d,mwhh,e

Phone Turn off please

Got it Wemo

I'm off now Wemo

Let's start an encrypted chat Wemo

api.xbcs.net Sure

iotowy;;s.gppr Wemo

api.xbcs.net smnvoeuu[

server, lets start an ecrypted chat. Wemo

Bugsense Sure

iotowy;;s.gppr Wemo

Bugsense smnvoeuu[

Phone Turn on please

Got it Wemo

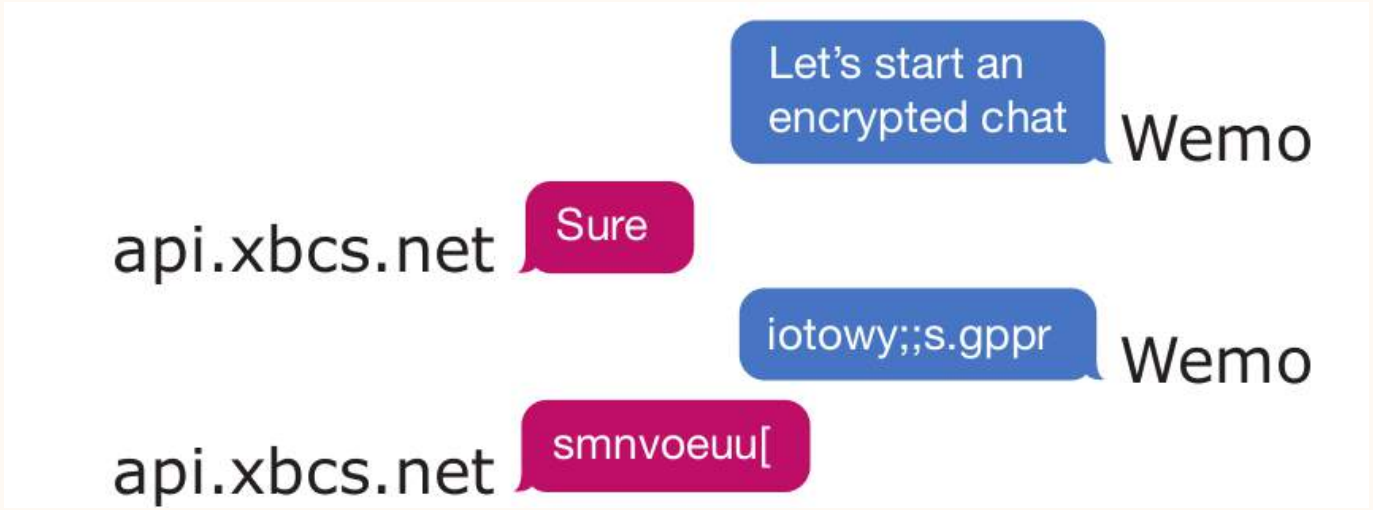
I'm on now Wemo

Phone Turn off please

Got it Wemo

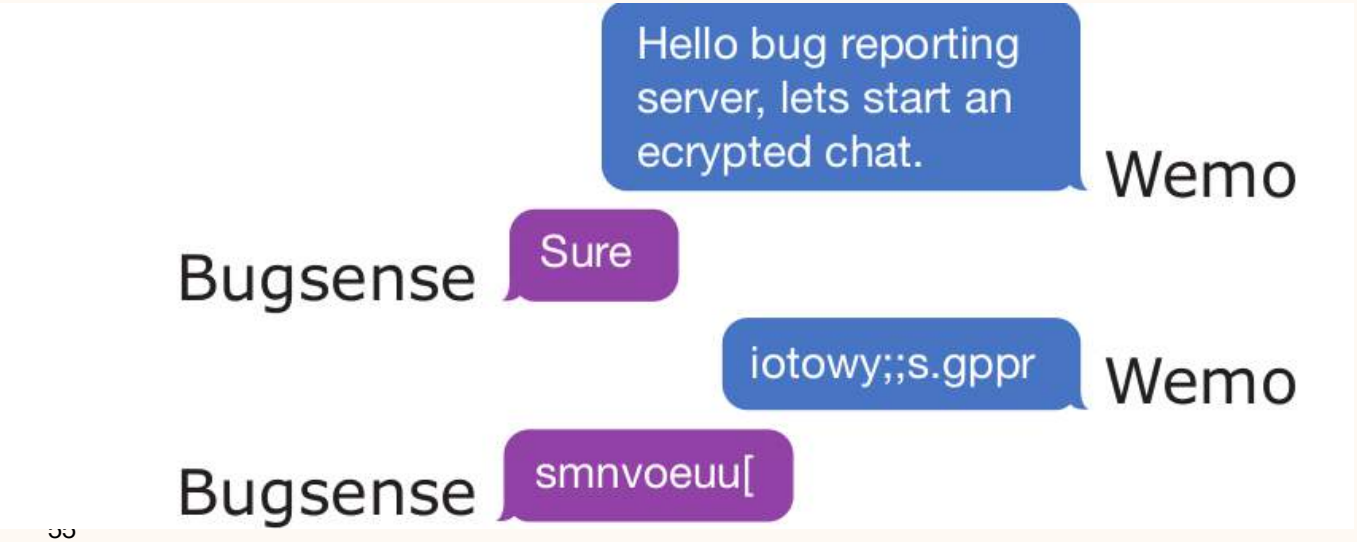
I'm off now Wemo

Sends some data (encrypted)



Talks to phone (local)

Reports a bug (encrypted)



14 IoT devices + apps

105 sites contacted

64% connections unsecured

37% could be secure if the developer made one change

Take-home

- **(Blog)** Lau, J., Zimmerman, B. and Schaub, F., 2018. Alexa, are you listening? Privacy perceptions, concerns and privacy-seeking behaviors with smart speakers. *Proceedings of the ACM on human-computer interaction*, *2*(CSCW), pp.1-31.
  (Blog) Mozilla – Privacy not included – smart home