Internet of Things & Surveillance

Overdrive Conference // April 2019
Barbara Wimmer // Twitter: @shroombab

Internet of Things

- Why do I talk about that topic?
- Background: IT-Journalist since more than 13 years
- cert.at Team >> Refridgerator that sent out spam mails (2014)

Structure of my talk

- Hacker Surveillance
- Surveillance Capitalism
- Corporate Surveillance
- State Surveillance

The „S“ in „IoT“ stands for „security“.


fb.com/ubook
Ein Service der universität wien
Merlin@home
Transmitter
ST. JUDE MEDICAL


Wi Fi


Vibratissimo
Vibratissimo


SCHUTZHAUS
PATSCHERKOFEL

The Good

- IoT is an extremely large field where you can do research on in terms of security
- There are opportunities for security consulting in a lot of areas (porn, sex toys,.. :-))
- Manufacturers react on reported issues

The Bad

- Risks can be catastrophic
- We are still in the beginning
- Future cyber operations will include an increased emphasis on changing or manipulating data to compromise its integrity to affect decision making, reduce trust in systems or cause adverse physical effects.

  Bruce Schneier in: Click Here To Kill Everybody. Security and Survival in a Hyper-Connected World. 2018.

Surveillance Capitalism

Surveillance capitalism is the monetization of data captured through monitoring people's movements and behaviors online and in the physical world.

(Shoshana Zuboff)

Surveillance Capitalism

We are living through the most profound transformation in our information environment since Johannes Gutenberg's invention of printing in 1439. And the problem with living through a revolution is that it's impossible to take the long view of what's happening.

(Shoshana Zuboff)

Corporate Surveillance

- Monopolies: Amazon, Google, Facebook
- Huge Data Collections
- Data should be owned by people, not companies


MEDION

Digital Assistant Corporations know…

- Who you talk/write to
- When you leave your house
- When you wake up in the morning
- What you shop
- What music you are listening to and what films you watch
- When you go to sleep
- What you are interested in

What happens with the data?

- Amazon, Google, Apple, Microsoft:
  - All digital assistants send all voice controls that are made after „Ok Google“ or „Alexa“ to their servers in the USA. The data will be stored there.
  - Will be used in the future - e.g. for advertisements
  - And will be shared with third parties after we consent through some XXX pages document and click.

DO YOU TRUST YOUR DIGITAL ASSISTANT? LISTENING TECH JOINS THE PRIVACY DEBATE

Counter Measures

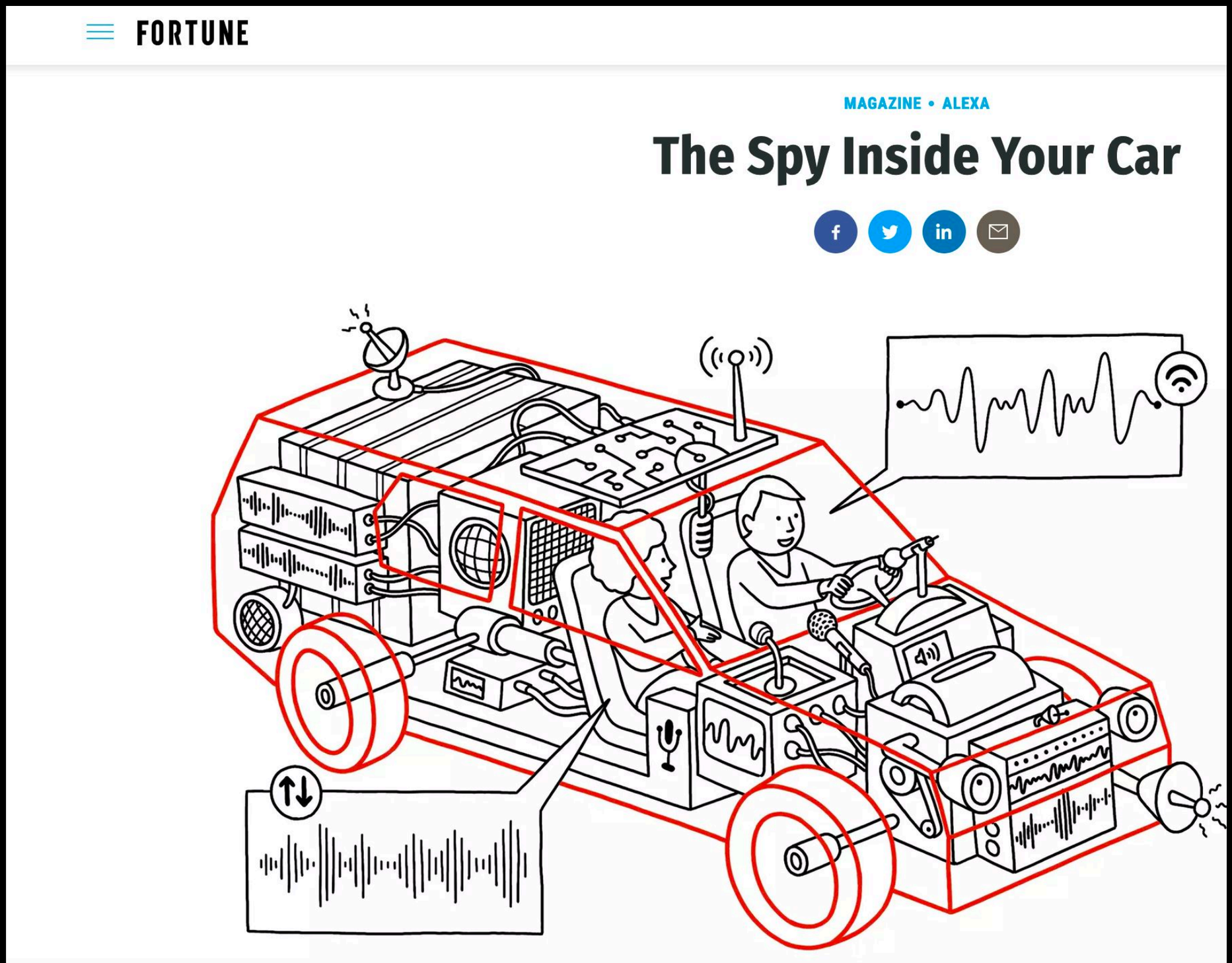
- Check the „Settings“ to control or delete the data that is collected (we don’t know on how many backup servers the data will be saved anyway)
- Use obfuscation methods: Don’t personalize your assistants too much. Use one or more dummy accounts to connect the device
- Otherwise: Don’t use them at all. It is your choice!

Amazon employs people to listen to Alexa conversations

Counter Measures

1. Open the Alexa mobile app
2. Tap the Menu button in the upper-left of the screen
3. Go to Alexa Account > Alexa Privacy > Manage how your data improves Alexa
4. Turn off “Help develop new features” and “Use messages to improve transcriptions” for all profiles on your account

Digital assistants are going to be everywhere



Who spies on us?

Currently automakers say they get customer permission before they use the individual data they collect for marketing or share it with third parties. But they already use those datasets.

BMW shares the data it collects. “Let’s say the person is listening to certain music, and we know there’s a big concert, then we would probably give that to our salespeople to make an offer for a special ticket.”

Data sovereignty

The collected data from products should belong to the users, not the companies. The users should be able to give companies certain rights to use them.

Wait, who owns the data?

- Companies use marketing tricks to keep full control of their products.
- User does not own the product anymore, because it only works with online connections and/or subscription models.

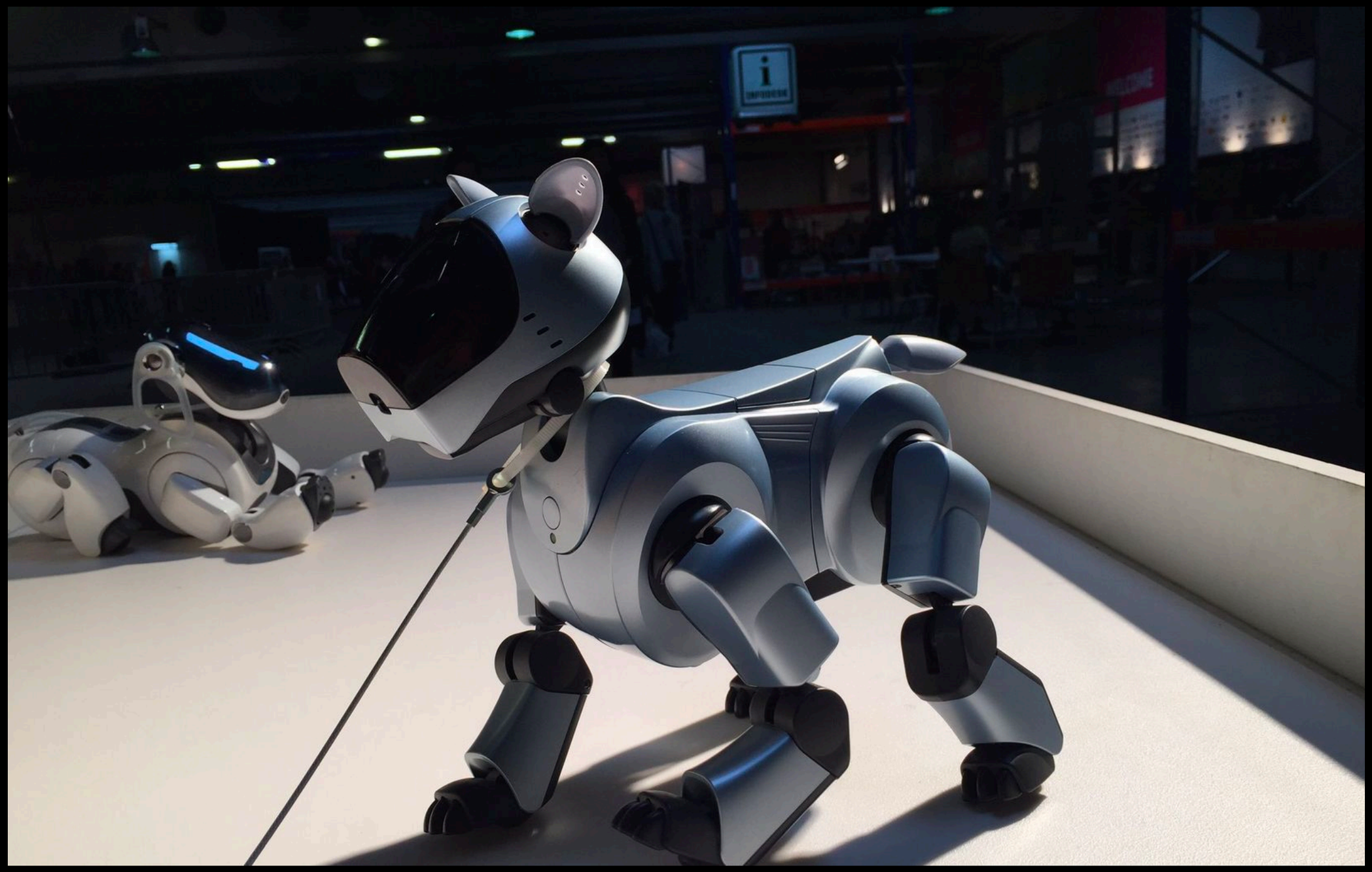
Nest Cam
- Surveillance Camera

- Camera does not work without an internet connection
- It is not possible to save the videos on your own computer (neither locally, nor in your own cloud)
- You have to pay to view the video content

Nest Cam - Surveillance Camera

YOU HAVEN'T CONNECTED YOUR NINTENDO ENTERTAINMENT SYSTEM TO THE INTERNET IN THE PAST WEEK. THIS GAME CAN NO LONGER BE PLAYED.

Aibo - Surveillance Dog



Farmers fight for their rights

DONATE

THE NEW FOOD ECONOMY
FOLLOW THE FOOD

TECH

As farmers fight for the right to repair their tractors, an antitrust movement gains steam

Ownership

Proprietary tools and restrictive user agreements keep farmers from fixing their own machines.

If you can’t repair it, you don’t own it!

Right to repair

- Consumer and business goods that once were semi-repairable with a manual and a set of tools now come stocked with proprietary digital software.

- Law could change the situation. We need a right to repair!

- Opposing the law in the US are currently companies like Apple and Microsoft.

State Surveillance

- Some countries take surveillance to an extreme, using the Internet to spy on the entire population. China leads the way: the country's social media platforms are all monitored by the government, and offending statements can be censored.

- Aside from surveillance, many countries use the Internet for censorship and control of their citizens

(Bruce Schneier in: Click Here to Kill Everybody)

Surveillance laws & internet

Austria:

It will soon be mandatory for big internet platforms like Facebook, Twitter and newspaper websites to register their users and deprive those behind postings of anonymity.

It would be up to the platforms themselves to decide the form of registration, but authorities would be able to access users' identities in case of hate postings or on suspicion of other laws being broken.

Surveillance laws & internet

Austria:

Proposal of a new „digital tax“ law:

Digital Tax Control based on IP address

Austrian ISP association compared Austria with Russia or China

Surveillance laws & internet

- Great Britain: New law where clicking on terrorist propaganda once could mean 15 years in prison comes into force
- UN special rapporteur professor Joe Cannataci says: “It seems to be pushing a bit too much towards thought crime…the difference between forming the intention to do something and then actually carrying out the act is still fundamental to criminal law.”

When policy goes wrong…

- We need to bring technology and policy experts together
- Laws must be made by people who understand technology and are willing to learn
- Bruce Schneier currently sees „two cultures“ that do not talk to each other, or, even worse: „they simply act Asia the other does not exist“

Hack
the
system!

Thank you for listening!

Twitter: @shroombab // Mastodon: shroombab@mastodon.at
Website: shroombab.at - Mail: shroombab@gmx.at