Section 7

Privacy

sinead.barton@mu.ie

Personal Profiling

In the US, mortgage brokers were blending web-tracking data along with geographical and other demographic data, to easily infer race. This data mining helped brokers – or the marketing companies they hired – target minorities with "ghetto loans," sometimes couched in the "language of African-American."

WATCH YOUR MOUTH

Your Samsung SmartTV Is Spying on You, Basically

You may be loving your new Internet-connected television and its convenient voice-command feature—but did you know it's recording everything you say and sending it to a third party?

SHANE HARRIS 02.05.15 7:35 PM ET

In the Netherlands, Smart electricity meters were deemed unconsititutional as they could profile customers activities, the types of equipment in their house, and when to suggest replacement/upgrades

Personal Profiling

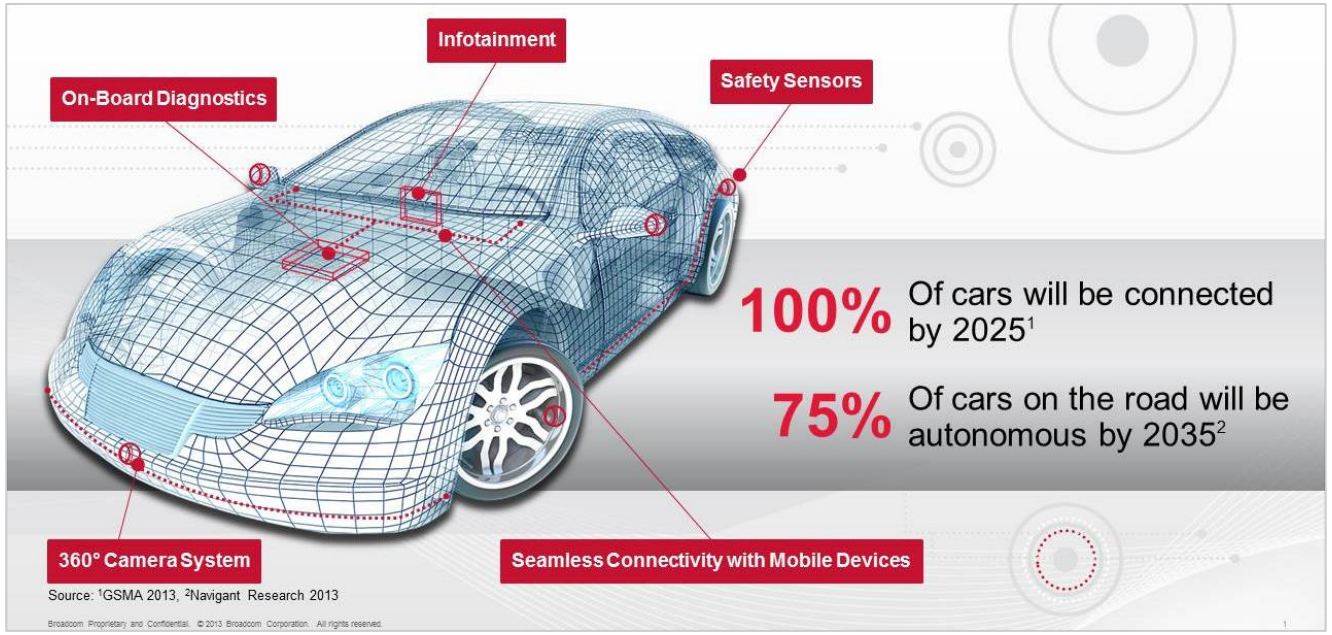
> **Would consumers be happy for insurers to look through their Facebook photos as part of the underwriting process? Or tracking their every move via a smartphone's location services to confirm whether their behaviour is in line with what they disclosed on the application form**
>
> RICHARD SADLER, HEAD OF RETAIL PROTECTION PROPOSITION DEVELOPMENT AT ZURICH UK LIFE

How Visa Predicts Divorce

By scrutinizing your purchases, credit companies try to figure out if your life is about to change—so they'll know what to sell you.

NICHOLAS CIARELLI 04.06.10 6:44 PM ET

Personal Profiling



- Recording everything that you do, how fast you go, where you go, with who?
- How valuable do you think this will be?

Where is this data stored?

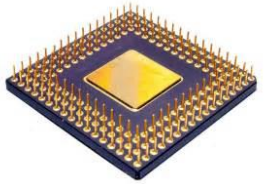
The problem is that "intelligence" is a computationally hard task to do properly

Putting all that "intelligence" in your product is likely to be very expensive, power hungry, and still likely impossible.

For this reason it is necessary to use the cloud.

“Cloud

“Connected”



“Intelligent Product”

Why does it happen?

- So you need to record all your data, and you send it back to the “cloud” for processing and the answers are returned. **Do what you need locally and send as much as you can back to the cloud.**
- So what do you do with all your recorded data when you are finished with it?

IOT Devices

Internet of things

What are IOT Devices?

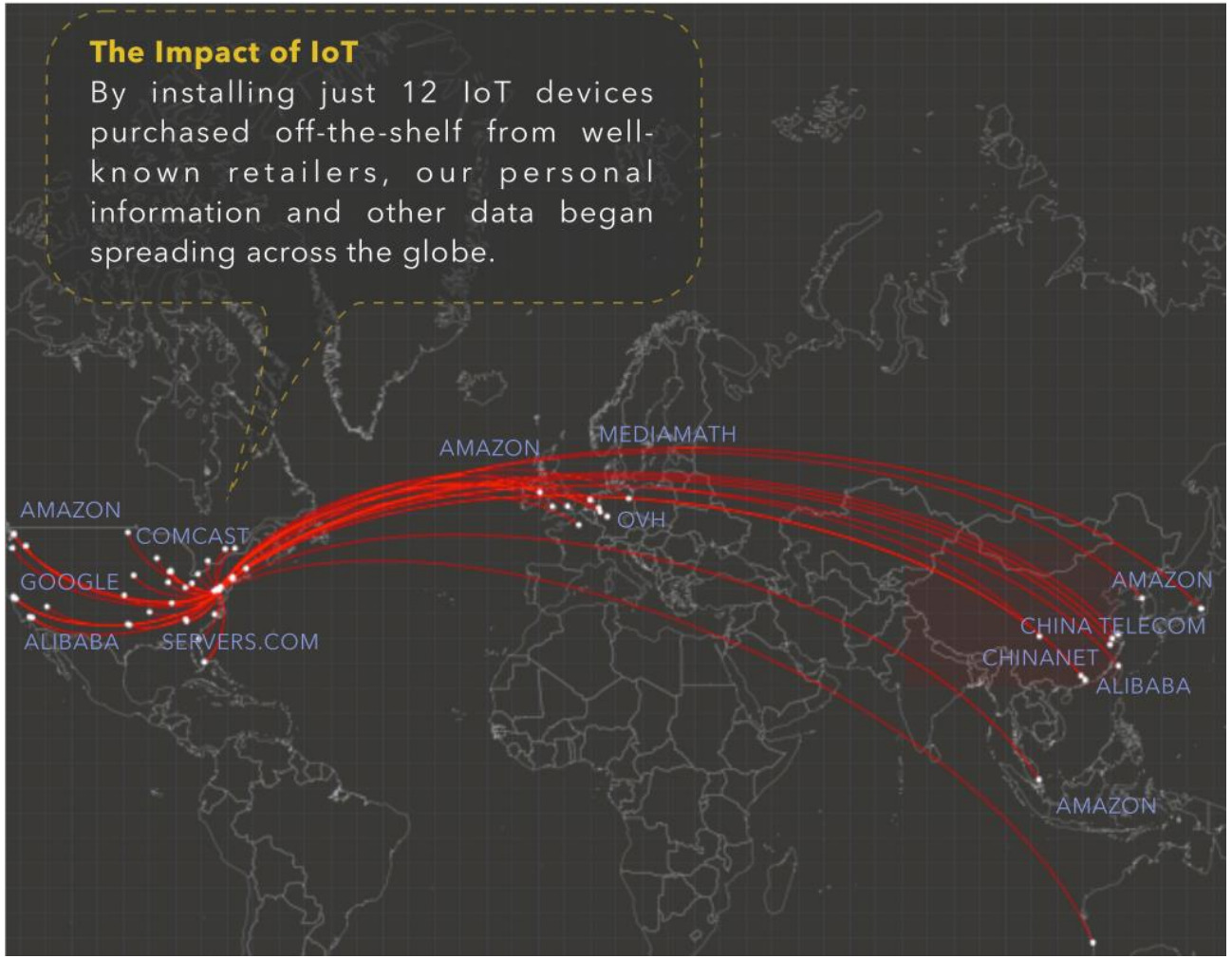
IOT devices are any device that has some form of intelligence and is connected to the internet.

Intelligence includes:

Sensors	Interacting with the environment it is in	Communicating real time data	Something that is controlled

A lightbulb that can be switched on using a smartphone app is an IOT Device

Trusting your devices



Trusting your devices

THE STATE OF IOT SECURITY

	Normal Permissions	Dangerous Permissions	Special Permissions	Not For Third Party Permissions	Hardcoded Password	Third-Party Domains	Vulnerable to Man-In-The-Middle	Access to Location Data
Guardzilla	9	8	0	4	!	11		●
iHome	5	2	0	0		11		●
MERKURY INNOVATIONS	7	6	1	0		40	●	●
momentum	7	5	0	0		12		
oCo	5	6	0	0		10		●
tp-link	8	4	3	0		17	●	●
VIVITAR	10	11	1	2		36	●	●
WYZE CAM	7	3	0	1		15		
zmodo	17	7	1	4		20	●	

Figure 5: Overview of Android application findings by device

The table above shows the number of permissions we found in each category as defined by the Android developers guide. It is important to note that it is typical for the average user tends to just accept permissions associated with an application upon install and to never consider them again.

What is personal data?

According to the European Commission "personal data is any information relating to an individual, whether it relates to his or her private, professional or public life"

Generally anything that can help identify any aspect of a person's life.

- It can include:
  - Names,
  - Addresses,
  - Biometric data
  - Medical records
  - Photos,
  - Email address,
  - Bank details,
  - Posts on social networking websites,
  - Computer's IP address, web browsing records
  - Mobile phone records, location data
  - Products that a person owns

How it could be abused?

Identity Fraud

- Name
- Addresses
- Biometric data
- Photos
- Email address

Medical Fraud

- Medical Records

Financial Fraud

- Bank Details

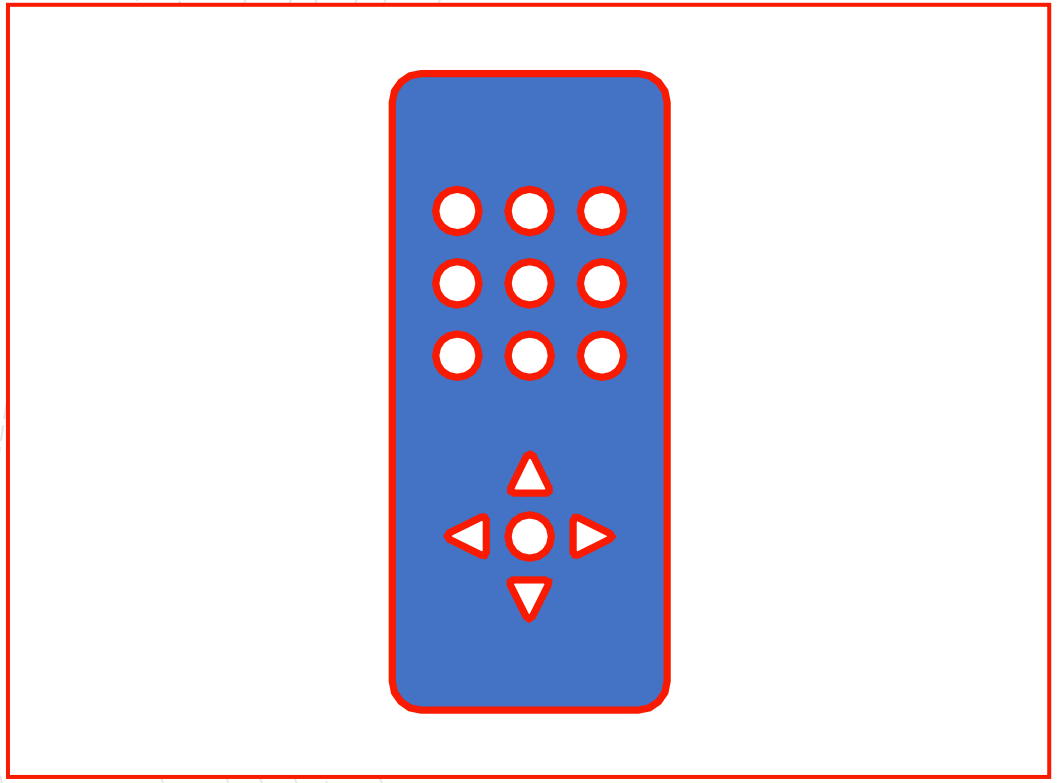
Limit Job Opportunities

- Posts on Social Media

Invasive Marketing

- Computer's IP address, web browsing records
- Mobile phone records, location data
- Products that a person owns

So are you able to control this?



Yes, but do you know if it's even happening?

Do you care? Will you ever care?

Around the world

For US Citizens

- Data privacy is a **consumer right** which is a weak category of rights
- **Narrow definition** of what is personal data
- **Low cultural sensitivity** to data breaches or data abuse
- No protections for non-US citizens

Around the world

- For EU Citizens
  - Data privacy is a **constitutional right** which is a very strong category
  - **Wide definition** of what is personal data
  - **High cultural sensitivity** to data breaches or data abuse
  - Rules apply primarily to all EU residents

EU's General Data Protection Regulation

May 2018

- The GDPR is the EU's way of giving individuals, prospects, customers, contractors and employees more power over their data and less power to the organizations that collect and use such data for monetary gain.
- It creates a set of new rights for individuals who provide data to organisations
- It creates a set of new obligations for organisations that collect data
- It applies globally to any organisation holding the data of EU citizens
- Breaches of the regulation can result in fines of up to
  - **€20 million or 4% of global annual turnover (whichever is greater)**

EU's General Data Protection Regulation

May 2018

- **Data holder obligations:**

- *Lawfulness, fairness and transparency*
  - Personal data must be processed lawfully, fairly, and in a transparent manner.
- *Purpose limitation*
  - Personal data must be collected for **specified, explicit and legitimate purposes** and not further processed in a way incompatible with those purposes. Consent must be given for the specific purpose and **cannot be used for other purposes without consent**.
- *Data minimisation*
  - Personal data must be adequate, relevant and **limited to those which are necessary** in relation to the purposes for which they are processed.
- *Accuracy*
  - Personal data must be accurate and, where necessary, **kept up to date**; every reasonable step must be taken **to ensure that personal data that are inaccurate are erased or rectified without delay**.

EU's General Data Protection Regulation

May 2018

- *Storage limitation*
  - Personal data **must be kept for no longer than is necessary** for the purposes for which the personal data are processed. Properly anonymised data may be retained longer

- *Integrity and confidentiality*
  - Personal data must be processed in a manner that ensures appropriate **security of the personal data**, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

- *Accountability*
  - The controller shall be responsible for and be **able to demonstrate** compliance with these principles.

EU's General Data Protection Regulation

May 2018

- **Consumer Individual Rights**

- **The right to access** –this means that individuals have the right to request access to their personal data and to ask how their data is used by the company after it has been gathered. The company must provide a copy of the personal data, free of charge and in electronic format if requested.

- **The right to be forgotten** – if consumers are no longer customers, or if they withdraw their consent from a company to use their personal data, then they have the right to have their data deleted.

- **The right to data portability** – Individuals have a right to transfer their data from one service provider to another. And it must happen in a commonly used and machine readable format. (big issue for people like Apple, Google, facebook)

- **The right to be informed** – this covers any gathering of data by companies, and individuals must be informed before data is gathered. Consumers have to opt in for their data to be gathered, and consent must be freely given rather than implied.

EU's General Data Protection Regulation

May 2018

- **The right to have information corrected** – this ensures that individuals can have their data updated if it is out of date or incomplete or incorrect.

- **The right to restrict processing** – Individuals can request that their data is not used for processing. Their record can remain in place, but not be used. There must be simple methods for withdrawing consent, including methods using the same medium used to obtain consent in the first place;

- **The right to object** – this includes the right of individuals to stop the processing of their data for direct marketing. There are no exemptions to this rule, and any processing must stop as soon as the request is received. In addition, this right must be made clear to individuals at the very start of any communication.

- **The right to be notified** – If there has been a data breach which compromises an individual's personal data, the individual has a right to be informed within 72 hours of first having become aware of the breach.

- **The right to the service** – there is no negative impact on the requested services if consent to processing is refused which is not necessary for the service being supplied.

Children

May 2018

- ‘Children deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data. This concerns especially the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of child data when using services offered directly to a child.’

- Article 8 requires that where the personal data of a child under 16 is being processed to provide ‘information society services’ (for example, online businesses, social networking sites and so on) **consent must be obtained from the holder of parental responsibility for the child**. Member states are allowed to lower this threshold where appropriate but not below the age of 13.

- If you are recording data about children, then you need to be super careful. **Children are unable to grant you consent to use their information**

- Ignorance is no defence

What does it mean for your design?

May 2018

- **SENSORS**
- Your intelligent device requires sensors to be aware of its environment – so you are collecting data

- For example:
  - The location of furniture in a specific persons house (eg robot-hoover)
  - The temperature settings in a house (eg temperature controls)
  - the voice of someone (eg kids toys)
  - Audio pickup in a room (eg Alexa)
  - Speed of travel
  - Location of the device (if related to a person)
  - Imagery (particularly of a child)

What does it mean for your design?

May 2018

GOOD

- If you **use and discard**, it is ok
- If you **use and store locally**, you are probably ok

BAD

- If you are sharing that data where it can be **accessed long-term or by other people**, then you must comply with the law
- If you are collecting and storing **more data than you need**, then it is illegal
- you must get permission to use the data for any **new purpose** or else it's illegal
- You can't **hide the consent request** in legal jargon (intentionally difficult language)

Obvious Conflicts

May 2018

- We said autonomous vehicles will require a "black box", how is that going to be managed?
- For many systems, e.g. medical, I need an audit trail, how do I handle that?
- How do you handle international transfers to regions working with different legal requirements?
- If I update my device to create a new "purpose", do I need to go back and ask for consent again? (YES)
- If someone hacks my product and accesses local storage – am I at fault? (potentially)

IoT News The Home

IoT Privacy: Roomba wants to sell maps of your living room. You shouldn't be surprised | WIRED UK

July 28, 2017 Mike Rawson Privacy, Roomba

The Internet of Things, a giant web of connected devices, is ever expanding and it's predicted there will be 8.4 billion connected items online by the end of this year. Fridges, toothbrushes, trashcans and even horses are being given the capability to connect to the internet. Every time another device comes online, more data can be harvested by its creators.

For customers, what's done with this data is largely unknown. iRobot, the company that makes the adorable Roomba robots that trundle around your home sucking up everything in their path, has revealed its plans to sell maps of living rooms to the world's biggest tech companies.

Some media articles

Some media articles

IoT News The Home

Internet providers could easily snoop on your smart home

August 30, 2017 Mike Rawson Security, Smart home

We've mostly moved past the point where our Internet of Things devices leak private information to anyone watching via unsecured connections, but that doesn't mean you can stop being afraid. *Never, ever stop being afraid.* To top up your paranoia reserves, a new study finds that internet providers can, if they so choose, monitor all kinds of things from your smart home's traitorous metadata.

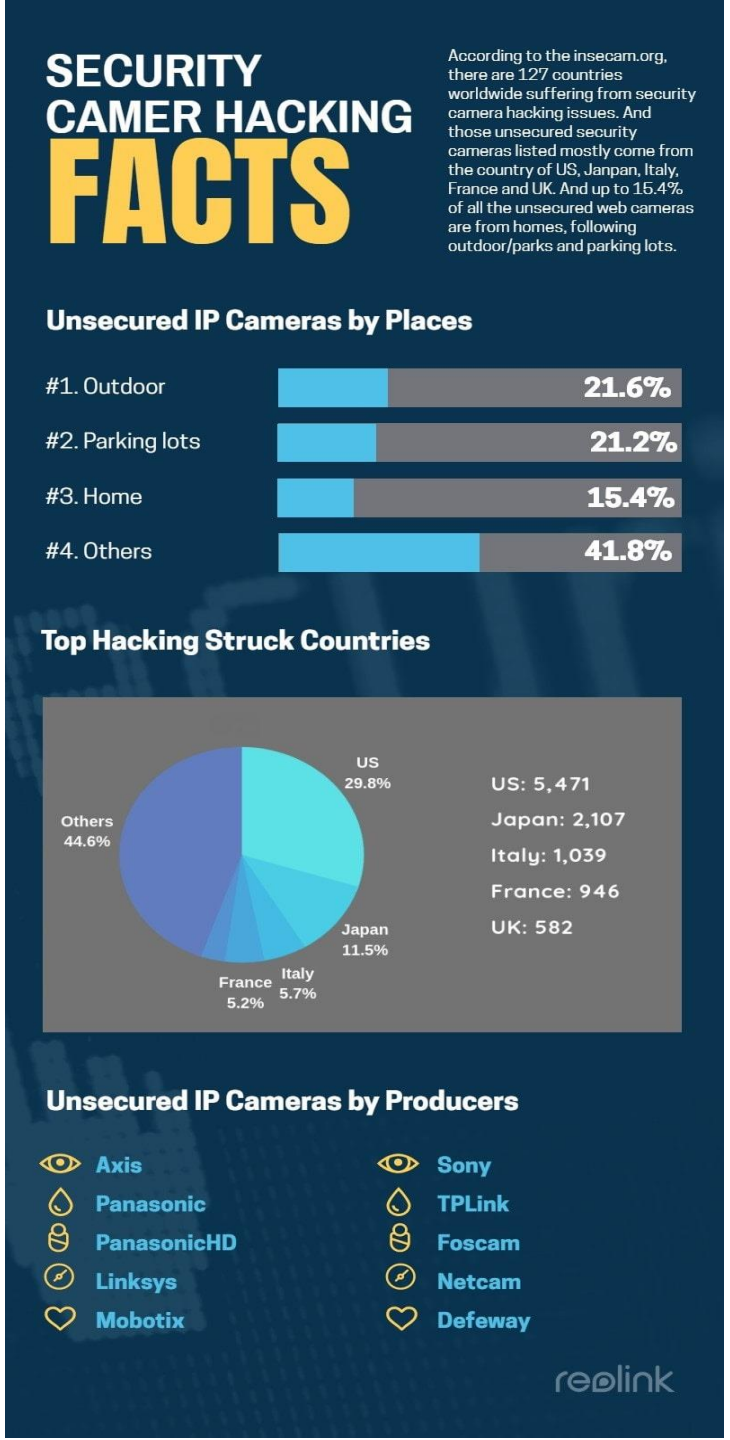
The paper, from a team at Princeton's computer science school led by grad student Noah Apthorpe, gets straight to the point: "we demonstrate that an ISP or other network observer can infer privacy sensitive in-home activities by analyzing internet traffic from smart homes containing commercially available IoT devices even when the devices use encryption."

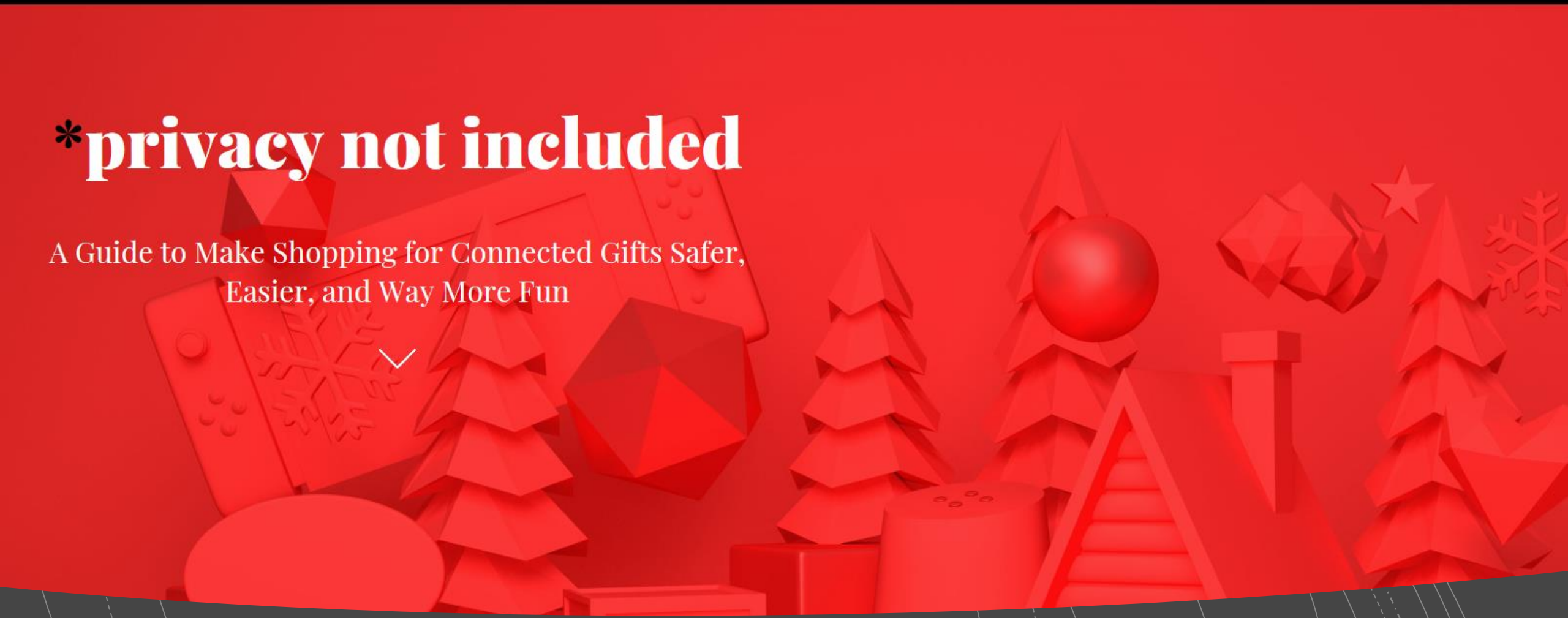
It's a pretty straightforward attack: the IoT devices often identify themselves voluntarily, usually by connecting to specific domains or URLs.

Unsecured Security Cameras

https://reolink.com/unsecured-ip-camera-list/

http://www.insecam.org/en/byrating/





Some Unsuspecting Products

https://advocacy.mozilla.org/en-US/privacynotincluded/

Ring

Ring Doorbell 2

$199.00

Door knockers are cool, but so old-fashioned. Door bells are neat, but so analog. Welcome to the future. Calling this a doorbell is a bit misleading. It's a door video, two-way audio, motion sensor, infrared night vision gizmo that lets you see, hear, and speak to people at your door from your phone or computer. But is it creepy? You decide.

Safety Review COPY LINK

Can it spy on me?

Camera	Yes
Microphone	Yes
Tracks location	Yes

What does it know about me?

Does the app require me to create an account?	Yes
Does it have privacy controls?	Yes
Can I delete my data by contacting the company?	Yes

Does the company share data with a third party for unexpected reasons?	Marketing

Some Unsuspecting Products

Some Unsuspecting Products

Sphero

BB-8 by Sphero

$149.99

"This is the droid you are looking for," says the website. Impossible to argue with that. Who doesn't want a little BB-8 droid they can control with their phone via Bluetooth? Or send the little guy out to patrol on his own. It also comes with something called "holographic simulation" which seems very important in helping the Resistance. Hopefully there is no Dark Side here.

Safety Review COPY LINK

Can it spy on me?

Camera	No
Microphone	Yes
Tracks location	No

What does it know about me?

Does the app require me to create an account?	No
Does it have privacy controls?	No
Can I delete my data by contacting the company?	Yes

Does the company share data with a third party for unexpected reasons? Advertising

Oral-B

Oral-B Genius Pro 8000

$249.99

Is Bluetooth the future of protecting your white teeth? That's the hope with this app connected toothbrush that "coaches" you up in your toothbrushing. Giving you real-time feedback if you're brushing all the right zones, with all the right pressure. No word yet on how many dentists out of five agree if this smart toothbrush is a smart buy.

Safety Review

COPY LINK

Can it spy on me?

Camera	Yes
Microphone	Yes
Tracks location	Yes

What does it know about me?

Does the app require me to create an account?	No
Does it have privacy controls?	No
Can I delete my data by contacting the company?	Yes

Does the company share data with a third party for unexpected reasons?	Advertising

Some Unsuspecting Products

Some Unsuspecting Products

Hatch Baby

Hatch Baby Rest

$59.99

Night lights used to be about keeping us safe from the scary monsters under the bed. Meet the "smart night light" that says it can help keep your toddler out of your bed. This Bluetooth night light connects to an app which lets you program when it turns on and off, what color it glows, and even plays soothing sounds to help the little one fall asleep. Hopefully it still protects from those monsters under the bed too.

Safety Review

COPY LINK

Can it spy on me?

Camera	Yes
Microphone	No
Tracks location	No

What does it know about me?

Does the app require me to create an account?	Yes
Does it have privacy controls?	No
Can I delete my data by contacting the company?	Yes

Does the company share data with a third party for unexpected reasons?	Advertising

FREDI Baby Monitor

The FREDI Baby Monitor fails in both Mozilla's security evaluation and user votes. This is not surprising since it has red flags all over it. For something that's supposed to keep an eye on your baby 24/7, its security (or lack thereof) is troubling.

For starters, the FREDI Baby Monitor doesn't encrypt its communications, it has no privacy policy and the company doesn't disclose if it shares information with third parties.

Some Unsuspecting Products

Default password is "123" so anyone anywhere can log in and find it

Some Unsuspecting Products

Bose $399.95

copy & share link

Bose QuietComfort 35 II

When it comes to pricey, high-end, wireless noise-cancelling headphones, Bose sets the standard. Worn by athletes, celebrities, and that guy next to you on the plane everywhere, these headphones do it all. They shut out the loud-talker on the bus, play music that sounds great, touch your ear to find Alexa or Google Assistant at your service, make voice calls, and tell the world you're doing well enough to afford a $400 pair of headphones. There's just one hitch, Bose was accused last year of spying--maybe even illegally wiretapping--users.

Small Homework

- Each group should identify one IOT device that they trust. Something that they believe to be secure and reliable.
- Send me a short message in Teams and tell me:
  - What is your group number?
  - What is the device that you trust?
  - Why do you trust it?
  - If your reason is because you understand technical details, would this be a problem for people who **do not** understand technical subjects?
- Send me your answers by 23.59, 20/11/30