The IoT Privacy Threat Landscape

NIST IoT Cybersecurity Colloquium

Dr. Gilad Rosner
gilad@iotprivacyforum.org
http://www.iotprivacyforum.org
Internet of Things Privacy Forum
@IoTPrivacyForum @GiladRosner
October 19, 2017

THE WILLIAM AND FLORA
HEWLETT
FOUNDATION

Research Project:

Internet of Things Privacy Risk Mapping

Investigators:

Dr. Gilad Rosner and Erin Kenneally

Research Design:

2 workshops (Bay Area, DC) with 27 invited participants. 17 semi-structured interviews. Thematic Content Analysis. Literature review.

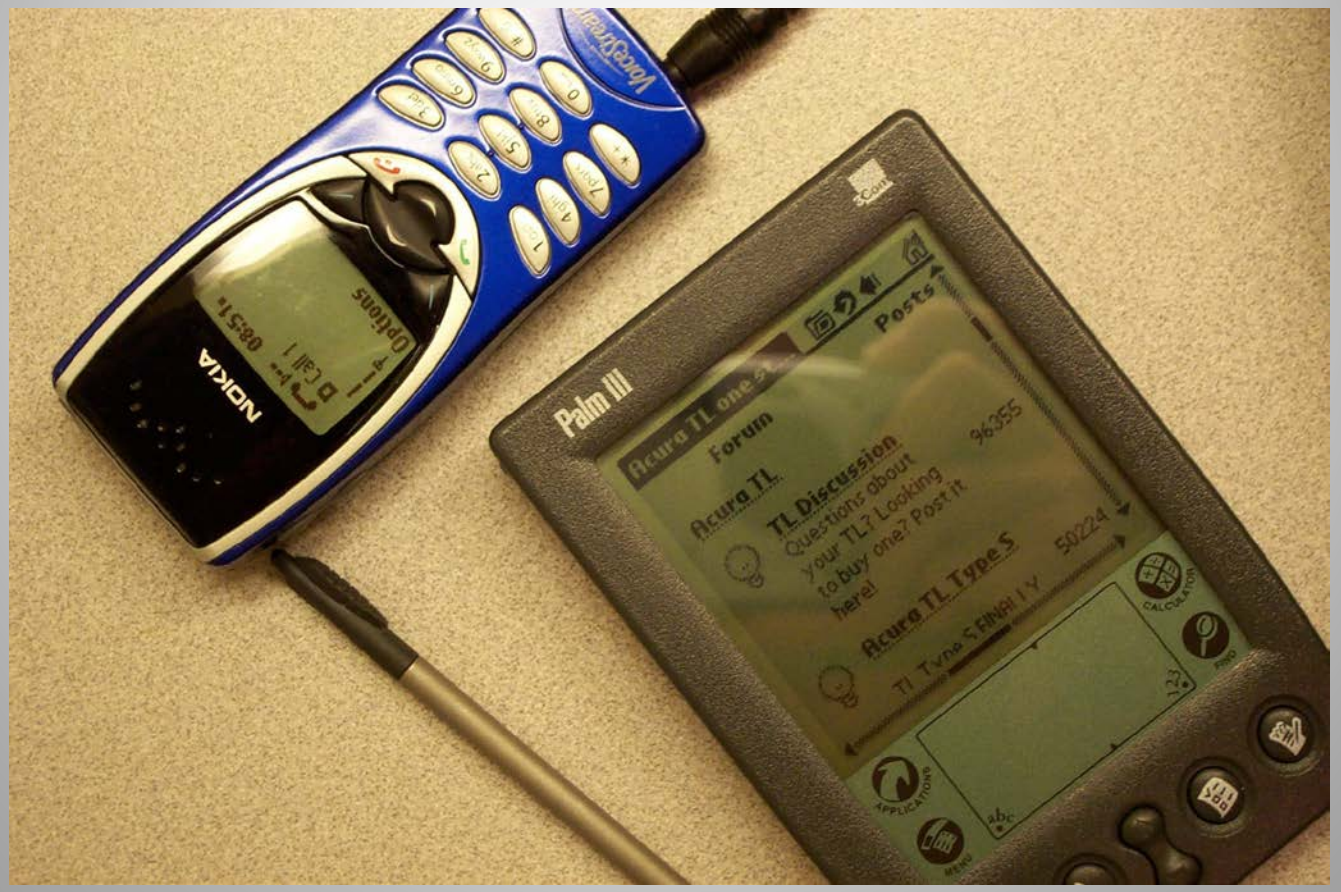
Defining the Internet of Things

Devices or Things are:

- not full-fledged computers
  - they are purpose-built items, versus generic computing platforms like your laptop, tablet and phone
- they have sensors, like cameras, microphones, infrared detectors, accelerometers, and much more specialized sensors
- they can communicate over networks
- they bridge the physical world with the electronic one
- in the consumer space:
  - gather personal data
  - tend towards being unobtrusive

~~“Internet of Things”~~

~~“Mobile Computing”~~?



The IoT allows the tracking and analysis that happens online to occur in the physical world

…the future of advertising and marketing lies in passive and always-on data collection, and that the Holy Grail is real-time information about customer needs and emotions. … Today this is dependent on advances in mobile and wearable technology, and correlation of geo-location with contextual and behavioral information. The value of passive data collection is instant access to transactions and conversations… Seen this way, biosensors and biometric data promise additional real-time understanding as people move throughout everyday life, the city and retail spaces.

- McStay, A. (forthcoming/2018) *Emotional AI: The Rise of Empathic Media*.

Diminishment of private spaces


amazon
amazon

Categories of Microphone-Enabled Devices		
	Description	**Selected Examples**
Manually Activated	Devices **begin** recording and transmitting audio only when manually switched on (by remote or button) and **stop** recording automatically or when the button or remote is released.	**Samsung TV** **LG Smart TV** **Sony Android TV** **Apple TV** **Fire TV** **Hello, Barbie**
Speech Activated	Devices **begin** recording and transmitting audio only after the microphone detects a "key word" and **stop** recording automatically after a short amount of time. Until then, they remain in an inert state of buffering and re-recording, allowing the microphone to passively "listen" for a key word without recording or transmitting information.	**Amazon Echo ("Alexa" or "Amazon")** **iPhone 6S ("Hey, Siri")** **Google Chrome ("OK, Google")** **Microsoft Cortana ("Hey, Cortana")** **Motorola X Phone (customizable)**
Always On	Devices **begin** recording and transmitting audio when turned on, and are designed to **continue** recording and transmitting data 100% of the time or until manually turned off.	**Nest Cam** **Baby monitors** **Kapture** **OrCam**

- Gray, S. (2016). Always On: Privacy Implications of Microphone-Enabled Devices


70°
Good morning!
it's 6:30 AM
dismiss


CNN
"Alexa, play my video flash briefing."

I think you can put them in the context of IoT and ask, is for example us having devices in our homes that are maybe surreptitiously recording us or collecting and sharing information that we're unaware of, or even just the fact that they're in our homes recording, is that a violation of the idea that we are free from surveillance? From government interference? That in our homes, it is a private space? I think once that fundamentally that idea is challenged, then you have questions of is it possible to ever find a private space, and how necessary is private space to freedom of thought? I would answer that it's very necessary. It's at the core.

- Privacy Advocate, Interview

You think you're being observed, so you behave differently. There are also habituation aspects - you might behave differently at first, and then you kind of become attuned to the technology being there, so you become maybe a bit more laissez-faire in terms of how you behave. You forget that these devices are active, but that doesn't mean that you're not leaving digital traces of mundane behavior anymore, and this data can reveal information about your preferences, what you like, what you don't like, or your health, your family situation, your financial situation, all kinds of different things that people prefer to keep private.

- Florian Schaub, Interview

Bodily and emotional privacy

Informational privacy encompasses physical privacy. The latter can refer to insulation resulting from natural conditions such as walls, darkness, distance, skin, clothes and facial expression. These can block or limit outputs and inputs. Bodily privacy is one form of this. This is seen in crossing the borders of the body to implant something such as a chip or birth control device or to take something from it such as tissue, fluid or a bullet.

- Marx, Gary T. (2012: x). Privacy is not quite like the weather.

We're seeing a net-rise of interest in sentiment and emotion capture. The industries are really wide ranging: from automobiles, insurance, health, recruitment, media, basically anywhere where it's useful to understand emotions…. In terms of kinds of industries that are really taking the lead on this, advertising and marketing is one of the obvious ones. Increasingly we're seeing retail move in to that area as well … all sorts of different sectors, ranging literally from sex toys all the way up to national security agencies, and all the marketing and organizational stuff in-between.

- Andrew McStay, Interview, emph. added

including biometric data about emotions to understand ‘brand levers’, or how to get people to act, click, buy, investigate, feel or believe. … [T]his objective involves ‘understanding people through all of their devices and interaction points, i.e. wearable devices, mobile and IoT’. In general, the aim … is to ‘collect it all’ so to build more meaningful interaction with brands.

- McStay, A. (2016: 4). Empathic media and advertising: Industry, policy, legal and citizen perspectives (the case for intimacy)

“interest in **emotional transparency**, or the unfolding of the body to reveal reactions, indications of emotions, feelings about brands, tracing of customer journeys and information that will help create ‘meaningful brands’”

- McStay, A. (forthcoming/2018, Ch. 8) *Emotional AI: The Rise of Empathic Media*, emph. added.

In a sense, perhaps it depends on your politics. You could say not very little. But, as a minimum, as a minimum, what's at stake is the capacity to understand people in richer ways than we haven't seen before. So certainly in the marketing and advertising context what's at stake is the capacity to get people to buy more stuff. So, when you talk about what underpins getting people to buy more stuff, essentially what you're talking about is the controlling and the manipulation of human behavior. In terms of what is at stake, as a minimum, nobody could disagree that **there's a better than average chance of raising the capacity to manipulate human behavior, typically in a consumer setting.**

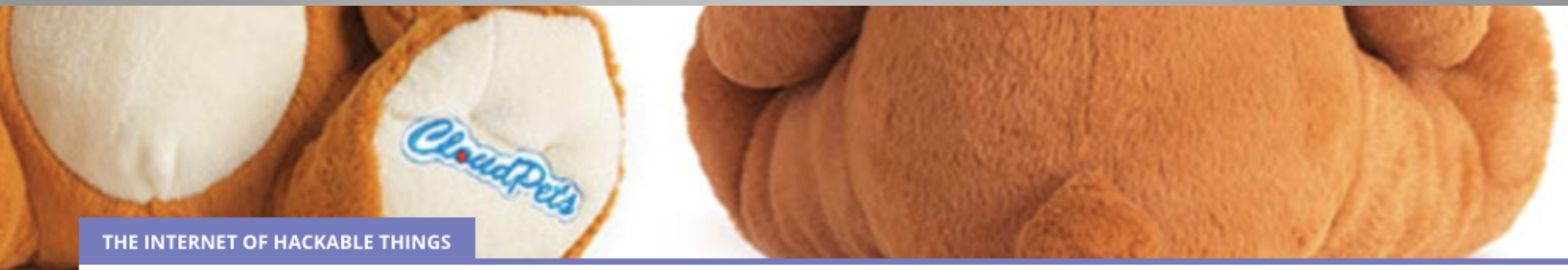
- Andrew McStay, Interview, emph. added

Children’s Privacy

German parents told to destroy Cayla dolls over hacking fears

17 February 2017 | Europe

The My Friend Cayla doll has been shown in the past to be hackable



THE INTERNET OF HACKABLE THINGS

Internet of Things Teddy Bear Leaked 2 Million Parent and Kids Message Recordings

LORENZO FRANCESCHI-BICCHIERAI
Feb 27 2017, 1:00pm

A company that sells "smart" teddy bears leaked 800,000 user account credentials—and then hackers locked it and held it for ransom.

UPDATE, Feb. 28, 12:25 p.m. ET: After this story was published, a security researcher revealed that the stuffed animals themselves could easily be hacked and turned into spy devices.


HELLO
HELLO
HELLO

Barbie is an iconic toy that people remember… She is really intended to be a peer… When you… set her up, one of the first things that she says is that you're one of her best friends and that she feels like she can tell you anything. She, through her design, creates this really intimate and important role in a child's life, both through those kind of big statements, "You're my best friend, I can tell you anything," but also we know that Barbies are kind of powerful. If someone says, "I can tell you anything," you don't expect that [the] intimacy that comes from a statement like that [to] also usually mean, "I'm recording everything you're saying and posting it on an internet platform that can also be viewed by your parents who can share it onto their social media sites."

- Legal scholar, Interview

Threat inflation: “the use of fear-inducing rhetoric to inflate artificially the potential harm a new development or technology poses to certain classes of the population, especially children, or to society or the economy at large.”

Technopanics: “a moral panic centered on societal fears about a particular contemporary technology … instead of merely the content flowing over that technology or medium.”

“While cyberspace has its fair share of troubles and troublemakers, there is no evidence that the Internet is leading to greater problems for society than previous technologies did.”

- Thierer, A. (2013). Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle

Thank you!

Dr Gilad Rosner
gilad@iotprivacyforum.org
http://bit.ly/grosner
Internet of Things Privacy Forum
http://www.iotprivacyforum.org