Introduction to IoT

The size of the IoT is expected to be immense: by 2020, 20–50 billon things are estimated to be connected as part of the IoT, leading some to predict an investment of US$1.7 trillion by 2020.

Allows for increased automation or action-at-a-distance.

IoT's informational and communicative functions have direct physical impacts.

A physical target accessible through cyberspace is more preferable for attackers than one that must be physically accessed.

General consensus that the security of the IoT is worryingly underd-eveloped.

The interconnection, via the Internet, of computing devices embedded in everyday objects, enabling them to send and receive data.

Informed Consent

A woman buys a vibrator, uses it, and discovers the company that built it is tracking just what she does with it and how often. And yes, she's suing.

A U.S. woman sued the company upon learning that the maker was "collecting information about her and other users' preferred vibration settings, the dates and times the device is used, [and] the email addresses of [device] owners who had registered their devices . . . [obtaining] all this data without the permission of its users"

People have the right to receive information and ask questions so that they can make well-considered opinions.

Stakeholders need to know what they are assenting to, and the "informed" part adds that component.

Informed consent requires something short of that, like knowing that some drug may cause nausea—exactly why the drug causes nausea is not necessarily so important.

EULAs: Tend to be too detailed, often running several pages filled with technical and legal jargon that is inaccessible to many users. Furthermore, the sheer length and density of these documents virtually ensures that users do not read them, instead clicking anything to make them go away.

Apple has 56 pages of terms and conditions. No one is going to read that!

As a way to deal with these issues, various commentators have proposed regulatory frameworks. Interestingly, this might come full circle to the medical context discussed from the outset as the sensit-ivity of personal medical data intersects with IoT applications, like Fitbits, Apple watches, and so on.

Privacy

Gathering information can lead to profiling and undesired targeted communication.

Target mined a client's purchasing habits, predicted that she was pregnant, and send a mailer promoting baby items to her home. As it turns out, she was still in high school and, while she was in fact pregnant, her family did not know; they literally found out because of the mailer.

Even if the data is encrypted, the metadata can nevertheless reveal pertinent details.

Consider something like Amazon Echo which, by design, is always listening.

Smart homes are routinely communicating information back to manufacturers, not all of which is even encrypted.

Reveals the resident's personal life or practices.

The European Union's GDPR just went into effect in mid-2018 and makes substantial strides toward increased data protection. Courts have also started to recognize rights to digital privacy.

IoT creates the perfect opportunity for gathering incredible amounts of personal information; that information can significantly bear on an individual's privacy.

Information Security

Many IoT components have sensors coupled to communicators. For example, a camera, microphone or other sensor picks up data from the environment and is coupled communicator that relays that data to a remote location, like the cloud or some proprietary server.

Smart televisions and other smart devices have sent data picked up by cameras and microphones from people's homes back to the producer's servers for analysis.

The lack of information security in the communications themselves has led to IoT-connected devices being used as part of distributed denial of service (DDoS) attacks.

Strava, a fitness-tracking app, is revealing potentially sensitive information about military bases and supply routes via its global heatmap website.

Default passwords to devices pose a threat

Heightened security impacts the very thing that the IoT is supposed to provide: seamless and invisible integration into our working and personal lives.

Physical Safety

Consider a smart home with a door lock that is activated when the user—or, more likely, the user's smartphone—is within five meters of the door.

The sensors and communications only serve their purpose when they cause some physical change in the world.

Should the driverless vehicle malfunction, its passengers, those in other vehicles, and the aforementioned cyclists and pedestrians may all be at risk.

Government oversight and enforcement of minimum safety standards.

New technologies, first and foremost, need to be safe.

"Safety in IoT means being able to reason about the behavior of IoT devices, especially actuators, and being able to detect and prevent unintended or unexpected behavior"

With the IoT, the causal networks are complex, and determinations of liability can be quite complex

What distinguishes the IoT from the traditional internet is the former's ability to act in the physical world, thus opening the possibilities of physical risk.

Trust

"Trust tends not to be talked about very much. Most of the time, it is an invisible assumption."

Can we rely on the technology to do what it is expected to do?

Given past experience, can we expect this technology to act the same way as it has done before?

Insofar as we rely on the driverless vehicle to work, we trust that the brakes are working properly and that the car will stop whenever that is needed. If this does not happen because the brakes malfunction, then we lose trust in that we can no longer rely on the car to operate properly.

We lose trust in that service when we do not expect the remote operator to drive the vehicle safely.

We can lose trust when we do not believe that people inside the company are motivated by our best interests.

Continuing with the example of driverless vehicles, in order for these individual vehicles to operate effectively, there will need to be coordination between the vehicles. The complexity of such coordination will likely require AI not just for the decisions made by discrete vehicles, but also for the complex system as a whole.

Trust (cont)

If and when the IoT involves significant risk to people's safety, and it can be shown that humans make worse decisions than AI, then we have a prima facie argument that AI should be making these decisions.