ITU Consumer protection in the digital age, Data Privacy and Protection: Webinar for Pacific Island Countries

Virtual meeting | 23 November 2021, 11:00 to 13:00 (+7 GMT)

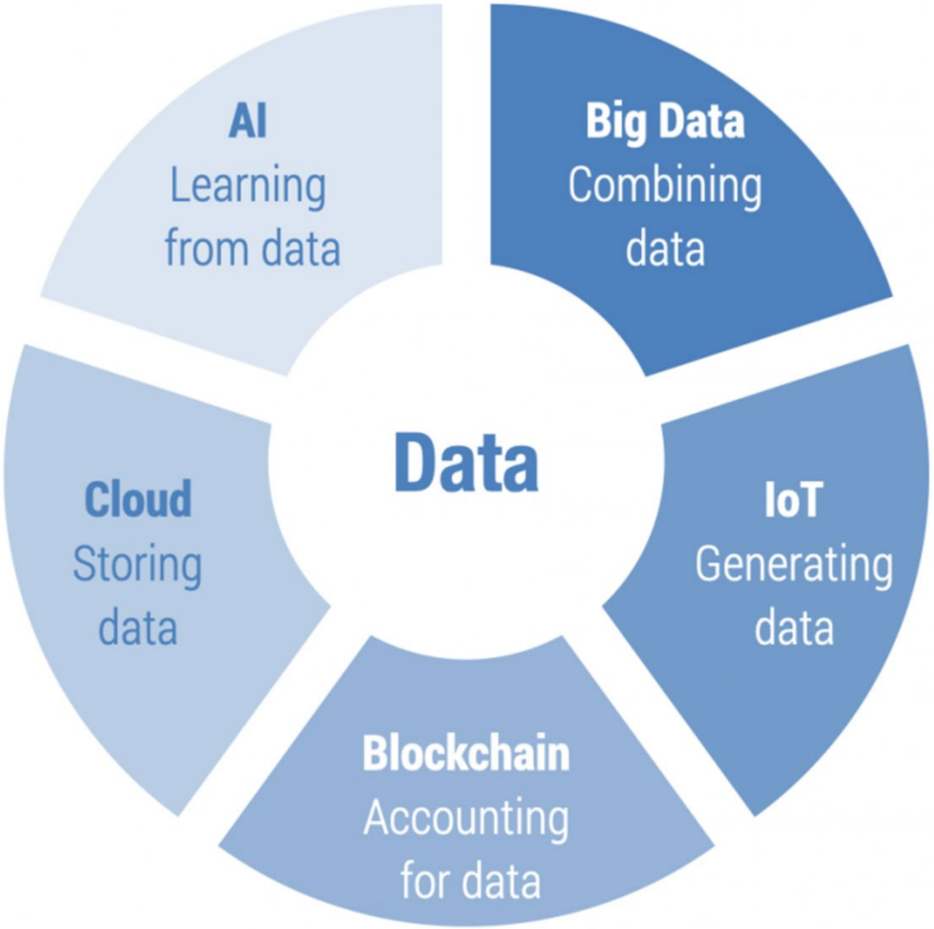
New technologies and their impact on consumers

Dr. Miriam Stankovich, Senior Digital Policy Specialist, DAI

Emerging technologies

Blockchain, AI, big data, the cloud, and the IoT all deal with data and that they facilitate new business models that may shift value creation within and between segments of the value chain.

- ❑ The IoT generates data (sensing and collecting)
- ❑ The cloud stores and processes data
- ❑ Big data derives data by combining large data sets
- ❑ AI learns from data, including big data
- ❑ Blockchain is a mechanism to reliably capture a data transaction history in a distributed manner



What is this presentation about?

- Unpredictability and changing nature o business models based on emerging technologies
- Liability
- Power imbalances and information asymmetries
- Data ownership, privacy, and security
- Benefits to consumers
- Key issues to be addressed and the way forward

1. Unpredictability and changing nature of business models based on emerging technologies

If a ride-hailing company, such as Uber, begins delivering food, it can fall under the jurisdiction of health regulators. If it expands into delivering drone services, it will fall under the purview of aviation regulators.

If it uses self-driving cars for passengers, it may come under the jurisdiction of telecommunications regulators.

Maintaining consistency in regulations is difficult in the sharing economy where the lines between categories and classification of services and products are often blurred.

2. Who is liable?

On March 18, 2018, at nearly 10 PM, a self-driving Volvo hit and killed a pedestrian, a woman named Elaine Herzberg. Herzberg's death was the first pedestrian fatality involving a self-driving car.

The self-driving car was a test vehicle, a car that Uber was testing in Arizona. It could not figure out if the woman was a pedestrian, a bicycle, or another car, nor predict where she was going. Video showed that the driver, acting as a "safety backup", was not looking at the road at the time of the collision. Instead, she was watching an episode of "The Voice".

This accident triggered Uber to temporarily stop testing their self-driving cars in Tempe, San Francisco, Pittsburgh and Toronto, and began a wave of legal action.

What obligations did the system's programmers have to prevent their creation from taking a human life?

And who is responsible for the death?

The person in the driver's seat?

The company testing the car's capabilities?

The designers of the AI system, or even the manufacturers of its onboard sensory equipment?

2. Who is liable?

- **3D printing** - If a 3D house crashes down, who is to blame — the supplier who supplied the design, the manufacturer who 3D printed the house parts or the manufacturer of the 3D printer?

- **Blockchain** – are smart contracts that smart?

Smart contract code could be especially problematic if it is used to deprive consumers of options and remedies in cases of fraud or deception, or if it otherwise permits one side to block legitimate defenses and operate above the law.

3. The use of AI and machine learning might generate power imbalances and information asymmetries

- **Targeted advertising.** The use of self-learning algorithms in Big Data analysis gives companies the opportunity to gain a detailed, individual insight into the customer's personal circumstances, behavior patterns and personality (purchases, sites visited, likes on social networks).
- **Price discrimination.** AI supports suppliers not only in directly targeting ads and recommendations to consumers, but in presenting them with individualised prices, and offering to each consumer an approximation of the highest price point that consumer may be able or willing to pay.

Consumers have direct interest in fair algorithmic competition, i.e., in not being subject to market-power abuses resulting from exclusive control over masses of data and technologies.

4. Data ownership, privacy, and security

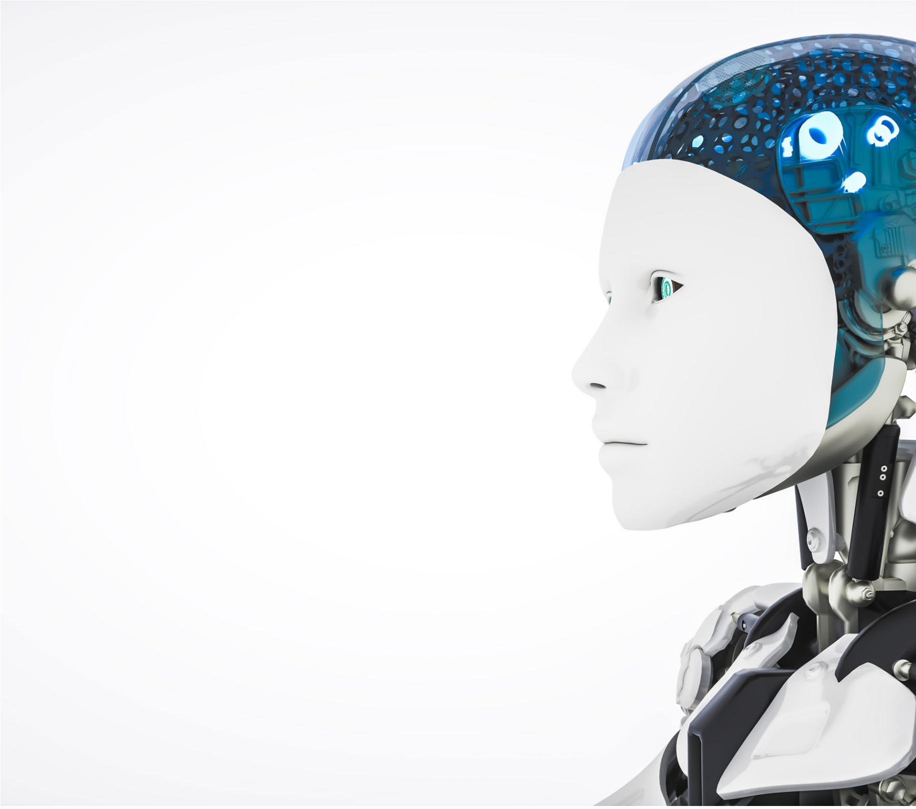
Who owns the data?

Privacy impacts data uses far beyond consumers' understanding

Sale and sharing of data?

Differences in regulatory approaches

Cybersecurity



IoT, smart devices and data protection: impact on consumers

- Data provided by a user to the service provider to have the service enabled
- Data generated by the user or associated devices as certain services are used

Should these two types of data be treated differently?

Device manufacturers qualify as Controllers for the personal data generated by the device, as they design the operating system or determine overall functionality of the installed software.

Third party app developers that organize interfaces to allow individuals to access their data stored by the device manufacturer will be considered Controllers.

Other third parties are Controllers when using IoT devices to collect and process information about individuals. These third parties usually use the data collected through the device for other purposes that are different from the device manufacturer (e.g., an insurance company offers lower fees by processing data collected by a step counter).

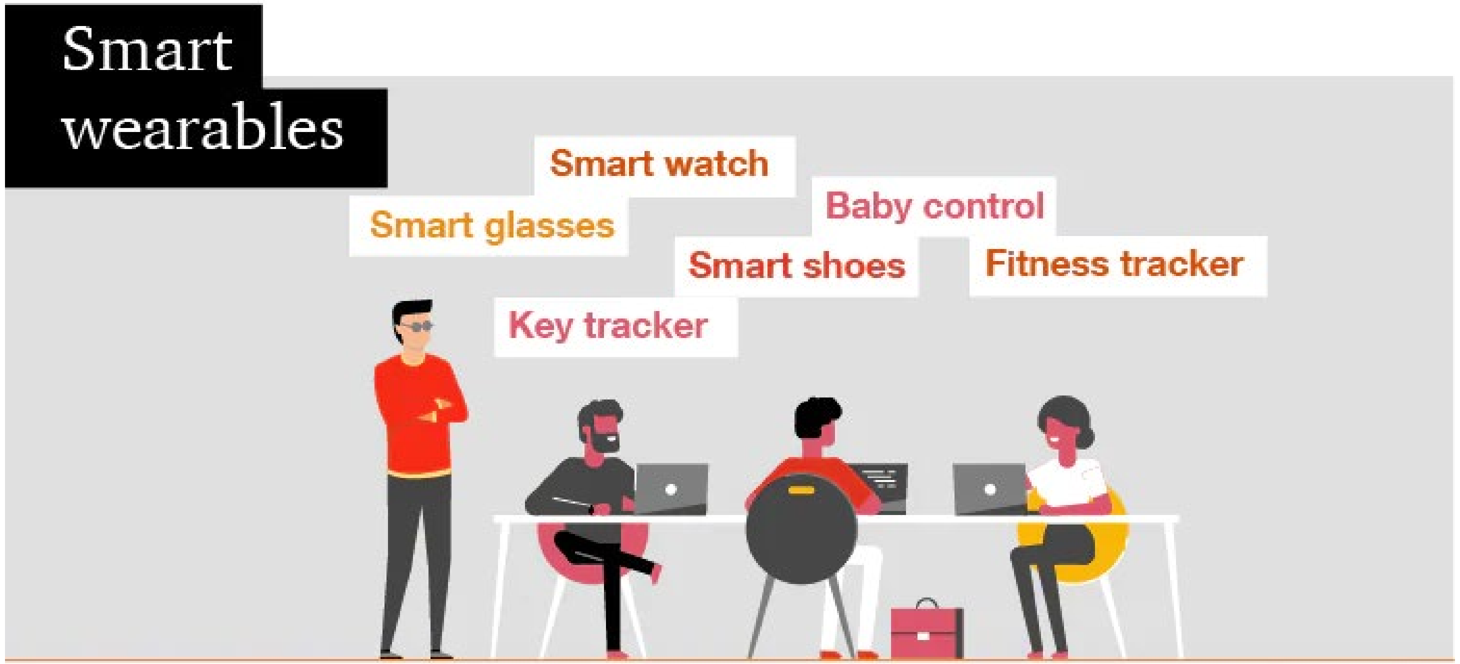
Other stakeholders such as IoT data platforms and social platforms may also be considered as Controllers for the processing activities, for which they determine purposes and means. On the contrary, they may be considered as Processors where they process data on behalf of another IoT stakeholder that acts as a controller.

IoT & data protection

The case of smart wearables

- To what extent are the companies who monitor health-related data under an obligation to disclose that data to the subjects they belong to if, for example, they reveal certain negative health conditions?

- To what extent can companies use this data for secondary purposes?

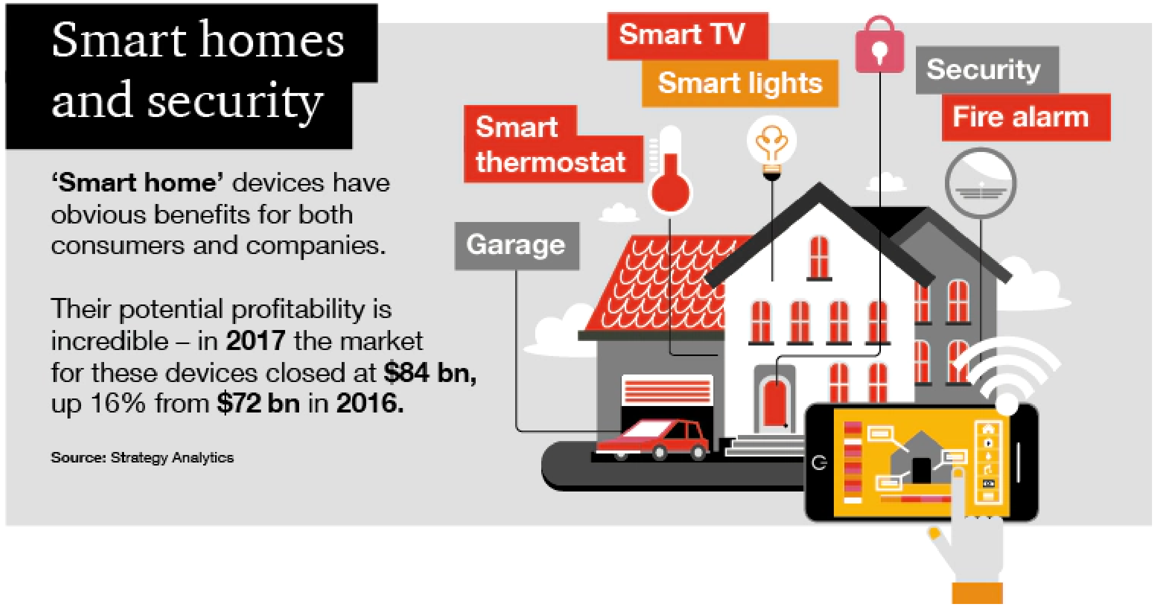


Source: PwC

IoT & data protection

The case of smart homes and security

- What is the extent to which the producer of one smart device may be to blame for the failure of another?
- If, for example, a smart fridge can be hacked and bypassed to unlock a connected smart lock, to what extent should liability for the economic loss of items stolen from the home be distributed between the manufacturers of each product?
- Depending on how these issues are tackled, there may potentially be significant risk, as a single weakness in the code could potentially be applied to thousands of products written with the same code.



Smart homes and security

'Smart home' devices have obvious benefits for both consumers and companies.

Their potential profitability is incredible – in **2017** the market for these devices closed at **$84 bn,** up 16% from **$72 bn** in **2016.**

Source: Strategy Analytics

Source: PwC

5. Benefits to consumers

Future "personalized" information – based on customer preferences, needs, capabilities, by way of analysis massive data stored by the business – could pave the way to more individualized products and services avoiding the one-size-fits-all rule.

Consumer organizations could use chatbots to provide useful information to consumers about their rights and the services available to them.

Key issues to be addressed by regulators and policy makers and the way forward

- The extent to which algorithmic price discrimination is acceptable in online markets should be clarified.
- Inacceptable practices in targeted advertising and nudging directed to consumers should be defined and addressed.
- Discrimination in ads delivery should be countered.
- Citizens and consumers should be provided with effective ways to turn off personalization.
- The development and deployment of AI tools that empower citizens and consumers and civil society organizations should be incentivized.

Thank you ☺

Dr. Miriam Stankovich

miriam_stankovich@dai.com