A device does not know its users’ voice: it can collect and storage voice data, images or information of third persons (other family members or guests) without them being aware of it.

Besides those data directly and consciously fed to the device by us, devices include sensors to catch and store other data, including images and audio.

Many companies that take part in the service provisions (device manufacturers, software developers, service providers, etc.) could access our data and process them for further purposes.

Combining collected data with information from other users allows to obtain information regarding our habits, behaviour and/or physical status.

Some devices can track our movements, and, at the very least, they can locate us at a certain point, over a certain period of time.

The sheer volume of data ant its combination with information from other devices allows to elaborate accurate profiles of our habits, preferences and device usage.

Even when we are not directly and consciously interacting with a device, it can still be collecting and processing personal data.

Any Internet-connected device with default insecure settings or unresolved vulnerabilities can become the access gate to cyber criminals in search of exploiting our personal data.

Personal data are processed by third parties who, in case of undergoing a security breach, may be exposed.