LIÈGE université
FACULTÉ DES SCIENCES APPLIQUÉES
Ecole d'ingénieurs et d'informaticiens

LIÈGE université
Droit, Science Politique & Criminologie

DROI1357-1
EUROPEAN LAW, (BIG) DATA AND ARTIFICIAL INTELLIGENCE APPLICATIONS SEMINAR

Pieter Van Cleynenbreugel
Jerome De Cooman

Privacy in household robots

Brugmans Victoria
Champagne Loïc
Hubar Julien
Klapka Ivan
Latour Manon
Metens Elsa

Masters degrees
Academic year 2020-2021

Contents

1 Introduction

Lately, with the help of years of research, new devices have arrived in our households, these are the so-called IoT devices. In a futuristic not-so-far vision, we could also adopt robots companions, some of them are in fact already available on the market. They are capable of providing us great services, such as cleaning our house or giving us the weather forecast. But how do they work? What data do they need in order to give us these services? Why and how do these devices collect data? Is there a danger of piracy? By whom, how and for what? Has the European Union tried to protect Human rights in this regard? If so, how? This paper will try to answer these thorny questions.

The emergence of household robots and more generally of IoT devices goes hand in hand with artificial intelligence and machine learning algorithms. However, those fields of engineering function with the collection of a large amount of data. Indeed, for machines to become intelligent, they need to learn repeatedly. They need data; the more data they have at their disposal, the more efficient they become. Therefore, our IoT devices collect data thanks to the various sensors that they carry. However, the components needed to interpret such large amounts of data are usually too expensive, too large to be placed in our IoT devices. Thus, to overcome this problem, manufacturers use remote services called cloud. This sends the data recorded by the IoT devices to its owner's range.

This work is organized according to the following structure. First, section 2 explores the concept of household robot in order to derive a definition. Second, data collection is explained in more details in section 3. Then, various incentives leading to export data out of the robot or IoT device are discussed in section 4. Next, section 5 presents security issues. Section 6 follows by studying the legal framework applicable to privacy in household robots. Afterwards, a discussion as well as potential solutions are discussed in section 7. Section 8 concludes the paper.

2 Household robots

2.1 Important concepts

Before examining different kind of household robots, a few concepts should be defined in order to ensure a common understanding.

In its paper *"A definition of AI : main capabilities and scientific disciplines"*, the High-Level Expert Group on AI starts with a definition stating that *"artificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications)"* [1].

Arising from this definition, Internet of Things (abbreviated IoT) needs to be explicitly defined as well. IoT is a network of devices connected through the Internet, communicating together and exchanging information. Those devices are then able to process acquired data in order to trigger an action [2].
Citing Ali [3], *"the purpose of IoT is to expand the functions of the first version of the Internet by increasing the ability to connect numerous objects"*.

It can be expected from an intelligent agent to hold the ability to learn. This relates to the filed of machine learning. *"Machine Learning is concerned with the design, the analysis, and the application of algorithms to extract a model of a system from the sole observation (or the simulation) of this system in some situations (i.e., by collecting data)"* [4]. In [3], it is defined as *"any methodology and set of techniques that finds novel patterns and knowledge in data, and generates models (e.g., profiles) that can be used for effective predictions about the data"*.
Machine Learning is therefore a sub-field of AI, which enables the system to learn rather than having its logic hard coded from the beginning.

2.2 Approach towards a general definition

From [3], a robot can be defined as *"a mechanical device that can be programmed to perform tasks of manipulation and locomotion under automatic control"*. Furthermore, such robots can be equipped or not with AI.

A first global approach to household robots would be to described them as electronic devices that can be purchased legally and that are designed to help in a certain way people around their home.

When told about household robots, one could picture a humanoid robot that helps in various tasks in the house. Such a multi-skilled robot is not yet a reality, but it could become one within five to ten years. For instance, the company SoftBank Robotics aims at providing such robots in order to assist elderly people. Some required design

features have been identified. Among others, the height should be sufficient so that the interactions with the robot are smooth, meaning for example that the user does not have to lean forward excessively, or that the robots can reach objects on a table. The robot should also be able to move around in the house and grasp various objects. This involves a way of detecting human beings as well as detecting when there is a contact. The robot should finally be powerful enough to carry its own weight along with providing walking support if needed. The overall appearance is important since it will determine the degree of acceptance by potential users.

When faced with this kind of robots, several questions related to privacy can be raised. First, for example, when the elderly person is in the bathroom, the robot should of course stay outside. But what happens in the case where the owner is taking longer than usual, or if the robot hears some unusual noise ? What is the reasonable trade-off between privacy and assistance ?
In the same idea, when the robot encounters some specific problematic situations, one may imagine that the latter could be programmed to ask for help from a remote operator, who would then take control of the robot. What could happen if a malicious third-party was taking the control ?
Additionally, for the robot to be proactive, it has to constantly observe and record information about the elderly person. Therefore, how can the user be ensured that those pieces of information are not broadcasted ? [5]

Besides the aforementioned humanoid robots, other robots can be found. It has been shown that the robot expression is an important feature, along with its design, in order for the customers to have a positive perception of the robot. In [6], two main categories of household robots are identified : "welfare-oriented" robots and "robots with hygienic features". The first category echoes the preceding paragraph, but it is not limited to it. There exists a wide panel of telecare robots such as robots with functional arms to help disabled people to carry out several tasks, exoskeleton robots to help people with reduced mobility, sentinel robots to ensure security, and other assistant robots such as Q.bo[1] or Care-O-bot[2].

Regarding the hygiene and cleaning of the house, one can think about the well-known vacuum robot, for instance Roomba by iRobot[3]. Among those vacuum cleaners, we can differentiate the ones using artificial vision and the ones relying only on sensors to detect collisions. Indeed, the former will map the house to optimize its path while the latter will go randomly around the room. A complete mapping of the house will thus be more likely to require a specific attention with regards to privacy. Other cleaning robots are available on the market such as robots for floor scrubbing and mopping. Moreover, we can include lawn mower, pool cleaner and window cleaner [6].

Among all the robots cited above, the extend of privacy threats depends largely on the level of intelligence given to the device, as well as its capacity to store and send data. Intelligence can be evaluated based on the rationality that a device presents, as well as its ability to learn.

[1]https://thecorpora.com/
[2]https://www.care-o-bot.de/en/care-o-bot-4.html
[3]https://www.irobot.fr/roomba

The concept of social robot is also relevant to our work. It is defined as *"physically embodied, autonomous agent that communicates and interacts with humans on an emotional level"*. This kind of robots aims at providing companionship, and hence psycho-social benefits, to the user. They rely on AI to be able to interact in a natural manner with their users [7].

As mentioned in the definition of AI, a system relying on artificial intelligence can either be a software, or can be part of a device. This is this second option that we will envision in the following. Those systems can be under multiple forms, going from the robots aforementioned to more common objects being added a sort of intelligence. The similarity lies in the fact that it needs "actuators", *i.e.* a mean to act on the surrounding environment. The actuators can be physical such as for robots (arms, legs, ...) or can also be a software as it is the case for IoT devices [1].

A field of application of IoT is what is called "smart homes". As part of those intelligent "things" entering the house, voice-controlled appliances can be mentioned [8]. Technically, the smart home is an IoT network connecting sensors, home appliances and smart devices through the Internet. The goal is to remotely control a residential environment, and automate various services such as lighting or heating to react to the household's needs [3].

2.3 Definition

From the discussion held above, we define a household robot as any device aimed at performing tasks within the house and its surroundings, that possesses a way of collecting or handling data.

Furthermore, robots that are studied in this work are considered as being equipped with AI, since they seems to lead to more concerning privacy risks.

In the context of studying privacy implications of those devices, a robot is thus to be understood as a broad term designating systems with sensors and actuators. It contains both the systems able to move and the systems for whose the actuator is a software without physical counterparty.

3 Data collection for household robots

3.1 What is data

In order to understand what data collection is, we first need to define what we mean by data. Data are characteristics or information, especially facts or numbers, collected to be examined and considered and used to help decision-making, or information in an electronic form that can be stored and used by a computer [9].

In this paper, we will focus our attention on data collected by household robots. Meaning that when we talk about data we mean data that has been gathered by a device setup around the house. This type of data can thus contain a wide range of different information and of varying importance. For example, the level of humidity of your basement captured by a smart air conditioner is considered data as much as the history of conversation you had with your Google home assistant.

In a legal perspective, the General Data Protection Regulation (GDPR) provides a definition of what is to be understood by personal data in its article 4 (1). It is *"any information relating to an identified or identifiable natural person ('data subject')"* [10].

The European commission in its White paper on AI stated that *"AI is a collection of technologies that combine data, algorithms and computing power."*[11]. As previously examined, AI systems can be used to thoroughly impact our society as a whole which is why users and European authorities need to be able to trust those systems. The European Commission therefore finds it crucial to ground AI in the Union's values as well as fundamental rights of which privacy protection is part.[4]

In other terms, AI systems must guarantee privacy and data protection throughout a system's entire lifecycle. This includes the information initially provided by the user, as well as the information generated about the user over the course of their interaction with the system (e.g. outputs that the AI system generated for specific users or how users responded to particular recommendations). Digital records of human behaviour may allow AI systems to infer not only individuals' preferences, but also their sexual orientation, age, gender, religious or political views. To allow individuals to trust the data gathering process, it must be ensured that data collected about them will not be used to unlawfully or unfairly discriminate against them.[11]

3.2 How is data collected

When it comes to household robots, many of them need to gather information from their environment in order to complete their mission. Whether it is for mowing the lawn or listening for a vocal command, household robots use what is mainly refereed to as a sensor to capture information about their surroundings. In the broadest definition, a sensor is a device, module, machine, or subsystem that responds to a physical stimulus (such as heat, light, sound, pressure, magnetism, or a particular motion) and

[4] Art 7 of the European Charter of fundamental rights and art 8 of the European convention on Human rights

transmits a resulting impulse (as for measurement or operating a control) [12]. Several types of sensors are often used together in order to gather more precise information.

3.2.1 Sensors

There is many different types of sensors. It would be useless to talk about all of them since there are too many, among which some are very specific. We propose here a list and explanation of the most common ones :

- **Light sensor** : Light sensors are a large category of sensors. They can range from simply being able to detect a change in luminosity to a full high resolution camera. The former is often used in combination with a reflecting mirror for detecting passage like stopping the garage door from closing if something is in the way, while the later can be used in a lot of different applications like smart doorbells or security.
- **Radio sensors** : Radio signal sensors are usually used in order to communicate over long distance by the means of radio waves. One of the most common use for radio signal sensors is for positioning purposes by using the Global Positioning System (GPS).
- **Temperature sensor** : This type of sensors can detect changes or even measure the temperature. It can be used in smart thermostat to adjust the level of heating in a house.
- **Humidity sensor** : A humidity sensor is used to measure the humidity level in a room and is usually coupled with ventilation in order to keep a place well ventilated like a shower or a toilet.
- **Electronic sensor** : This is a really broad category of sensors which allow to detect current or voltage going through a wire. It can be used to detect the activation of actuators or monitor electric consumption.
- **Electromagnetic sensor** : Electromagnetic sensors detect changes in electric and magnetic fields. They can be used to track movement of magnets or else variation in electric current. A fuse is an example of an electromagnetic sensor.
- **Liquid sensor** : This type of sensors can detect the presence of water or other liquids. It can be setup in certain areas of the house to alert you in case of flooding.
- **Gas sensor** : Gas sensors are used to detect certain types of gas like carbon monoxide or simply smoke and are often paired with an alarm system.

3.3 Why most household robots need data to operate

The simple answer is that it depends on the robot and its application. Most household robots gather information with the objective to successfully carry their mission. For example, a smart thermostat will keep track of the temperature inside the house in order to adjust the level of heating required.

Other use of sensors can be for security reason, such as a garage door coupled with a light sensor in order to avoid crushing something while closing.

Certain devices also have access to more data then they really need. For example, the webcam of a smart doorbell could record constantly while normally only be intended for helping identifying who is ringing at the door at that specific moment.

Data can also often be inferred from other type of data. This property can be useful for building robots, for example a smart lock might not need to calculated the angle of the lock to determine if the door is locked or not. It can simply turn the motor and detect if their is resistance, and thus simply checking if the lock is locked or not. Inference can sometimes unfortunately be used to obtain information that people would have like to remain private. A home assistant for example could listen for noise in order to detect if someone is currently in the house or not.

4 Incentives to export data

This section will explain why it can be advantageous to export (and store) data outside of the initial purchased device.

4.1 Improvement or development of products

In an ideal world, manufacturers would be focused on improving their product and making the user's experience as pleasant as possible. In this ideal world, the sole purpose of data collection would be to improve the product and the user's experience.

Therefore, to understand how and why data collection can improve these goals, it is necessary to understand some basic principles of machine learning. Indeed, in order for an algorithm [5] to learn, it needs a lot of data.

The main idea is basic, the algorithm randomly divides the input data into 2 categories: the learning set and the test set. Then, thanks to the learning set it will try to predict the test set data. This way, the programmers will be able to optimize the parameters of the algorithm in order to increase the prediction accuracy on the test set. Once the prediction rates on the test set are acceptable, the algorithm will then be able to predict new values that do not yet exist. As shown in the figure 1 below, the algorithm tries to predict whether it is an apple or a pear. We observe a first phase (on the left) during which the algorithm learns to recognize the characteristics of apples and pears. Once it has been trained, it is presented with a fruit and it is able to predict that it is an apple (on the right of the illustration). To be able to do this he has to recognize a lot of apples and pears. So it becomes understandable why so much data is needed.

[5] In mathematics and computer science, an algorithm is a finite sequence of well-defined, computer-implementable instructions, typically to solve a class of problems or to perform a computation. Algorithms are always unambiguous and are used as specifications for performing calculations, data processing, automated reasoning, and other tasks.

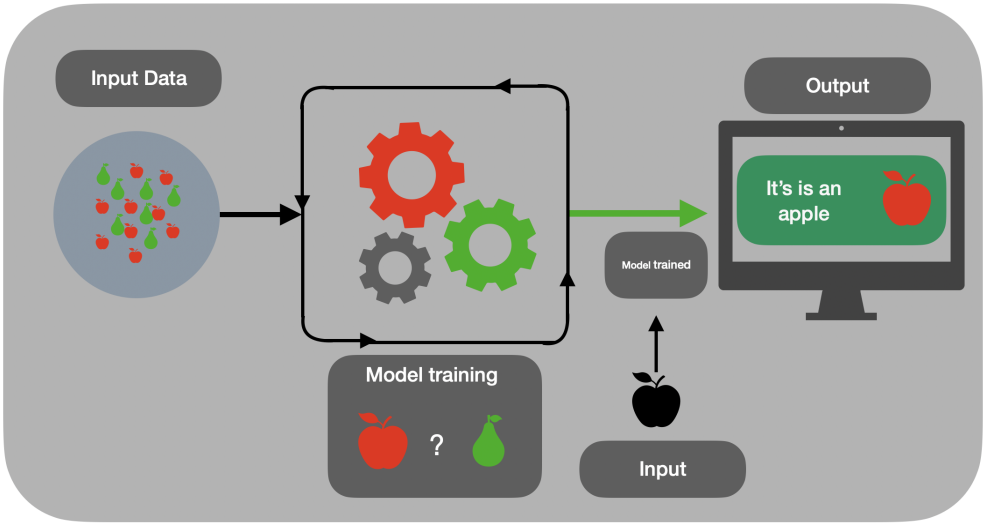

FIGURE 1: Illustration of operation of an machine learning algorithm

4.2 Remote help for computation

In an economy where the price of different technologies is constantly falling, manufacturers have no choice but to follow the trend. Therefore, they decided to dematerialize the operations of calculation, storage and maintenance. In order to perform calculation operations, a machine will need components that are relatively expensive and very often sensitive to heat, humidity and therefore susceptible to breakage. As a consequence, to overcome this problem, manufacturers have decided not to equip their machines with a lot of expensive and breakage sensitive pieces. They simply equipped their device with communication parts such as esp8266[6]. Able to send a request, a message to a computing unit.(see figure 2)

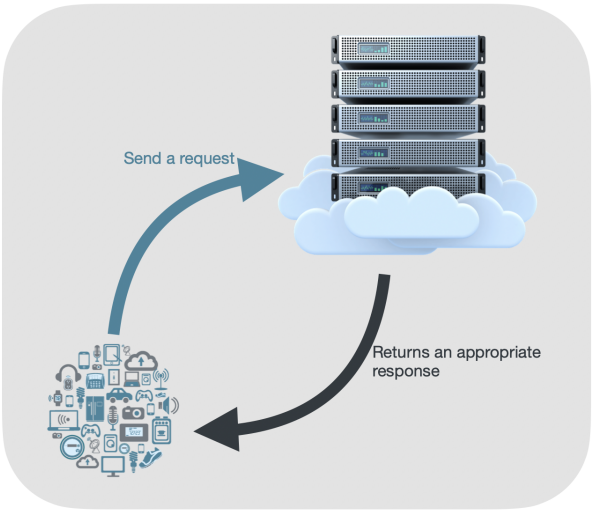

FIGURE 2: Illustration of IoT communication to the clouds

[6]The ESP8266 is a low-cost Wi-Fi microchip, with a full TCP/IP stack and microcontroller capability

In this way the manufacturers are free of two problems. Indeed, they can ensure that the environment in which the sensitive pieces are placed is as optimal as possible. Moreover, by centralizing the calculation operations, they can reduce the number of components needed for them as the sum of components needed to perform an operation centralized is less than the one needed to perform an operation decentralized. Moreover, by solving this last point, they also solve the maintenance problem at the same time. Since then, expensive pieces that need to be replaced and require the intervention of a technician can be done at the same place. Finally, the problem of data storage, as with computing units, requires expensive and breakable pieces. Moreover, data cannot be lost. This implies that data must be copied and stored in several places. Figure 3 illustrates how the majority of data is stored around the world.

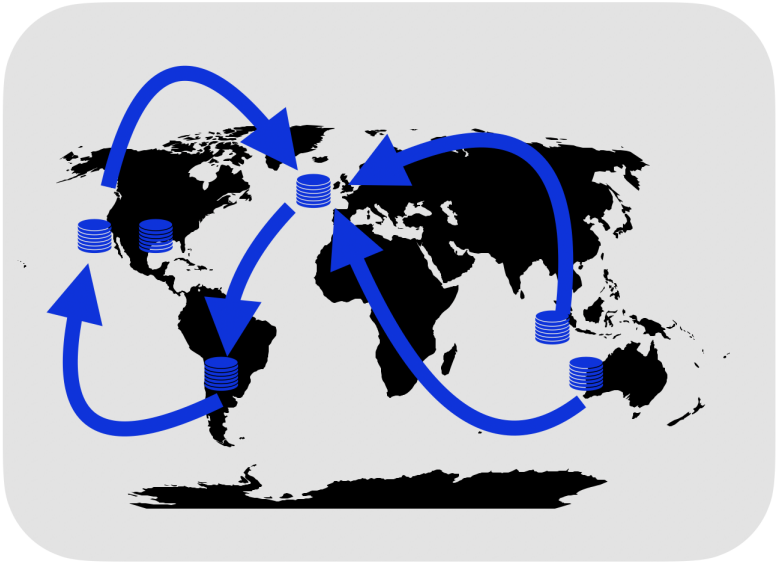

FIGURE 3: Illustration of server location in the world

5 Security issues

The IoT device industry is one of the fastest growing industry into the IT world. As a matter of fact, it is estimated that there will be more than 21 billion IoT devices by 2025 [13]. This huge number of device also comes with a number of new vulnerabilities. In a 2014 study [14], HP tested the top 10 popular Internet of Things (IoT) devices and found that 70 percent of them contained "serious vulnerabilities". On average, 25 vulnerabilities were found per device, totaling 250 vulnerabilities. Even if this study may seems quite old (6 years old), the observation made by this study seems to still stands nowadays. This means that if nothing is done by 2025, 14 billions of IoT devices will suffer from serious vulnerabilities.

These networked devices have access to data that can be intensely private, e.g., when you sleep, what your door lock pin code is, what you watch on TV or other media, and who and when others are in the house. Moreover, the state of the devices themselves represents potentially sensitive information. Because IoT apps are exposed to a myriad of sensitive data from sensors and devices connected to the hub, one of the chief criticisms of modern IoT systems is that the existing commercial frameworks lack basic tools and services for analyzing what they do with that information (i.e., application privacy) [15] [16].

The question that may arise now is: Why is there so many vulnerabilities with these devices ? Actually, Those vulnerabilities come from different factors. The two main reasons are firstly a question of money coupled with a lack of incentive to secure the devices and secondly a lack of shared standards between manufacturers.

In point of fact, IoT devices providers tend to diminish as much as possible the cost and the selling price of these devices. This implies that by diminishing too much the cost of these devices, the IoT devices have merely enough power to perform their main purpose and thus lack computation power to be able to line up with the security requirements [17]. Additionally, because IoT is a nascent market, many product designers and manufacturers are more interested in getting their products to market quickly, rather than taking the necessary steps to build security in from the start. Plus, as many IoT devices are "set it and forget it"[7] they hardly ever receive security updates or patches. From a manufacturer's viewpoint, building security in from the start can be costly, slows down development and causes the device not to function as it should. For example, adding security to a humidity sensor can make it unusable as the device will be too big or too costly (i.e. nobody would buy that device at that price point).

Finally, IoT security is also plagued by a lack of industry-accepted standards. While many IoT security frameworks exist, there is no single agreed-upon framework. Large companies and industry organizations may have their own specific standards, while certain segments, such as industrial IoT, have proprietary, incompatible standards from industry leaders. The variety of these standards makes it difficult to not only secure systems, but also ensure interoperability between them.

[7] placed in the field or on a machine and left until end of life

Unsecure IoT devices are detrimental for you and your family as developed in the `Section` 7.3, but also others. As explained in the paper [18], on October 12, 2016, a massive distributed denial of service (DDoS) attack left much of the internet inaccessible on the U.S. east coast. *"A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices"* [19]. This attack is commonly referred as the Mirai botnet attack and was performed by thousands of household IoT devices like smart refrigerators, security cameras and so on. Some may now wonder how do the attackers managed to take control over those devices. The answer to that is that the attackers began by targeting unsecure IoT devices by trying to access them with commonly used passwords like "admin", "123456", and others. Due to a lack of security, the attackers managed to gain access to a lot of devices. Afterwards, they installed a malicious software on those devices that make them (i.e. the smart devices) act like zombies bot. Zombie bot means infected devices that will try to infect new devices. This is how they managed to infect so many devices. Once infected, the attacker can send a message to those zombies in order for them to send network traffic to a victim in order to overflow the victim and make the victim service unusable by regular users. Unfortunately, this kind of attack can only be fully countered by securing IoT devices.

Now arises the question of liability. In the case of zombies into a business network, there is two possibilities :

- The company (IT Department) becomes aware of zombies within their network, such devices must be rendered harmless immediately to avoid liability : both criminal liability for aiding in computer sabotage ; and civil, if the injured party were to claim damages. Furthermore, in that case, the fact that the business IT is neither always perfect nor fully secure would not necessarily suffice as a viable defense against criminal, administrative, or civil liability.

- Secondly, and this is where it gets really interesting, businesses may be liable even without knowing that some of their devices are being used in a cyber-attack. Even setting aside the “critical infrastructures” in the European NIS Directive [20] and the rare cases of a possible criminal liability of the CIO for criminal omission of security measures, there is room for administrative and civil liability, especially now that the German IT Security Act [21] is in force. If the compromised system is intended for use by the public, e. g. a webserver, businesses must take all commercially reasonable measures to prevent any unauthorized access in order to avoid administrative fines of up to 50,000 Euros.

As for the question of liability in the case of household zombies, the law is not very clear. But, as suggested in this paper [22], the manufacturer should be held liable in that case. This should provide an incentive for the manufacturer for securing there devices.

6 Legal principles and Framework

6.1 Legal framework

The General Data Protection Regulation [10] is the legal document through which personal data is regulated in the European Union. It aims to protect Individuals' privacy by offering a framework for companies to rely on when collecting personal data.

The European Commission insisted on the trust any AI system should induce. The Ethics Guidelines for trustworthy AI bring up three crucial components that need to be respected and taken into account to create a Trustworthy AI system [23].

Firstly, The AI system needs to be lawful. In other words, it needs to comply with the current legislation. However, the Group of experts mandated by the Commission do not further examine this particular point.

Then, AI systems need to be robust. Indeed, individuals and society must feel safe when using AI and mustn't believe they could potentially be harmed by the technology. Artificial intelligence needs to function in a secure and safe atmosphere and provide with safeguards to prevent from any harm that could be caused by its malfunction or any unintentional impact. Moreover, robustness has to be technical as well as societal. It has to ensure that the environment and context have been taken into account by the system.

Finally, Artificial Intelligence has to follow Ethics guidelines. In order to believe in these new technologies and because the current legislation does not fully take into account the newest of technology, Ethics have to come in and fill the gaps left by the legislation.

6.2 Ethic principles

The group of experts takes therefore as a starting point the European fundamental rights from which they extract the Ethic values that need to be respected. The Fundamental rights identified by the Group of experts [23] are the respect for human dignity, the freedom of the individual, the respect for democracy, justice and the rule of law, solidarity as well as citizen's rights.

The Freedom of the individuals means that any human being should be able to make their own decision by themselves. Thus, they should all be protected against harm caused to their decision-making process, whether it be from the government or any another entity.

In light of the current boost in Artificial intelligence, Ethics principles have therefore been highlighted by the Group of experts mandated by the Commission. They pointed out four main principles [23] being The respect for human autonomy, The prevention of harm, Fairness and Explicability. In this paper, only the second ethic

principle, Prevention of Harm, will be discussed as it appears to be the one with the closest link to privacy protection.

6.2.1 Prevention of harm

When talking about AI systems, one could easily understand the positive outcome they have on society. Indeed, thanks to technology, our daily life is rendered a lot easier. However, that comes at a certain cost. In fact, AI can also be a source of risks that could harm juridically protected interests whether they are tangible or intangible. This is exactly why the ethics guidelines [23] state that no harm can be caused or exacerbated by the Artificial Intelligence through the prevention of harm principle. Doing so, the guidelines protect human dignity as well as physical and mental integrity of the human being. Therefore, it is crucial to create a legal framework that will protect users in their security and responsibility. A way of doing that could be by introducing obligations, imposed on Member States, that would take into account the intangible harm that could be caused to the user, especially to the more fragile one. If no regulation was to be taken concerning AI, organisations like OECD (Europe) or CNIL (France) state that AI systems have to be created in a way that respects the democracy values as well as diversity [24].

As privacy protection is a fundamental right of the individual[8] we can easily understand that violating the individual's privacy through collection of data, which is also protected by the article 8 of the European Charter of fundamental rights, could be considered as harming the mental integrity of the human being. In fact, as Public law Professor Alan Westin [25] said in 1970 in his treatise on privacy, People require alone time in order to process the emotional stimulation of daily life. Violating the individual's privacy could therefore, many believe, cause psychological harm. One of privacy's central roles in society is to help create and safeguard moments when people can be alone. In a certain way, by protecting mental integrity the guidelines protect the fundamental right to privacy as well [25].

Another way of protecting data and therefore privacy can be found in the GDPR [10]. In fact, the GDPR installs in its article 25 [26] the Privacy-by-design and Privacy-by-default mechanisms. These mechanisms will try to ensure a certain degree of data protection to the users and thus privacy protection as well.

In other words, as said by UK's Information Commissioner's office (ICO), *"The GDPR requires you to put in place appropriate technical and organisational measures to implement the data protection principles effectively and safeguard individual rights"* [27].

Indeed, on the one hand, the privacy-by-design mechanism consists in saying that AI technologies will have to integrate data protection from the design state and through the entire lifecycle, as stated previously in this paper. This concept of privacy-by-design already existed in the data protection law but is now a legal requirement [27]

[8] We can find it in art 7 of the European Charter of fundamental rights or the art 8 of the European convention on Human rights for example

thanks to the GDPR. This concept emphases on the fact that privacy protection and data protection have to be considered of utmost importance and have to be taken into account at the earliest stage possible, hence the Design stage and throughout the whole system's lifecycle. The GDPR states a few requirements in that area in order to fully reach the privacy protection goal. The requirements are the following: *"put in place appropriate technical and organisational measures designed to implement the data protection principles effectively; and integrate safeguards into your processing so that you meet the GDPR's requirements and protect individual rights"* [27].

On the other hand, the GDPR also takes into account and encourages the data protection by default. Such a mechanism relies on the fact that any individual should only have at its disposal the minimum information needed in order to achieve the goal which was set. It shouldn't be able to have access to more data, the data accessible should respect the proportionality principle and thus only the necessary information should be accessible [27]. If one looks at the article 25 of the GDPR [26], it states that the controller will be responsible for the compliance with data protection by design and by default. For instance, the AI developers will have to take into account those requirements in order to assist the controller.

As previously mentioned, the Ethics guidelines [23] state that no harm can be caused or exacerbated by the Artificial Intelligence. Furthermore, it is important to highlight that the environment in which AI is used needs to be free of danger. It needs to be protected from hacking as well as from unwanted utilisation. The robustness of the system is therefore more than encouraged, it has become an imperative. One could think of a recent problem (2019) that occurred in this specific area (Data protection). Indeed, a device which was sold by Lidl called "Robot Monsieur Cuisine" [28] created by Silvercrest was at the top of the tabloid in 2019. This culinary IoT device was equipped with an Android tablet which didn't take into account the specific use of the culinary robot and thus collected a lot more data than what was necessary in order to achieve the culinary goal. In fact, the developers incorporated a preexisting tablet which was not made for this specific culinary purpose and therefore collected a wide range of data. Two IoT professionals wanted to examine the cyber security of this robot. In order to do so, they tried hacking the robot and found it very easy to do so. One of them achieved connecting to the tablet and use it to go on the internet. Moreover, this robot was equipped with a microphone for vocal commands. The problem being that such microphone could also be hacked in order to listen in on the conversations of the family and potentially access important information such as bank information. The tablet was indeed complying with the data protection principles of the year 2015 but no update was made on this robot and thus the culinary device didn't comply with the new rules on privacy and data protection.

All in all, this example illustrates perfectly how important it is to ensure data and privacy protection from the start and throughout the entire life-cycle of the device.

6.3 Trustworthy AI

In order to achieve the creation of a trustworthy AI system, the group of experts of the European Commission has highlighted [23] 7 key requirements that need to be met by the technology. All 7 requirements won't be examined in this paper as they are not all impacting privacy as a whole. In fact, this paper will only examine privacy and data governance, Technical robustness and safety as well as Transparency.

6.3.1 Privacy and data governance

Firstly, privacy can be impacted if AI is used in an unwanted manner. The respect of privacy, which is a Human Right, is essential to live in dignity and security. However, in the electronic environment, in particular when using social networks or applications, a lot of personal data is collected, usually without the individual knowing, and can be used to establish a personal profile and predict our behaviour. In a way, we provide information on our health, our political opinion and our family life without knowing who will use such information and to what end.

The Ethics guidelines of the European Commission highlight that privacy is a fundamental right and that the prevention of harm to such privacy can be encountered by managing the data given as well as the way the data is collected [23].

A major problem in this area arises when talking about unjustified surveillance and mass surveillance. In fact, AI creates the problem of identification and tracking of individuals. For instance, in regards to facial recognition, using AI could mean that individuals' liberty could be diminished. They could be scared to utilise their rights and scared to be spotted by the cameras and to face consequences. This means that there is a potential risk of auto-censorship [29]. Having that in mind, the group of experts wanting to guarantee privacy specifies that in order to be considered a trustworthy AI system, in this particular context, there is a need to differentiate between simple identification and unjustified surveillance. While the first one could be used positively by the Police for instance, the second one is harming individuals' privacy. However, even in the first form, this technique isn't risk-free. Indeed, it could have a negative impact on psychological and sociocultural perspectives. Thus, it is of major importance that such techniques are governed by the current legislation. The experts mainly refer to the notion of consent of the individual.

6.3.2 Technical robustness and safety

Secondly, AI systems need to be robust and safe. They need to resist external attacks and unintentional impacts which could damage or manipulate the systems. A number of problems could arise when using an AI system in regards to the lack of security they provide. For more information, the reader can check the `Section` 5.

6.3.3 Transparency

Thirdly, AI will only be a success if it is trustworthy. The technical transparency implies that AI systems need to be auditable, intelligible and comprehensible to people from different backgrounds and different levels of expertise. For the group of experts of the European Commission, it is essentially the fact that AI systems have to be conceived in a way that permits their supervision [23].

If there is a lack of transparency, problems could arise as well. Mainly, it would be the black box effect that would cause damage. This effect consists in the fact that there is a certain degree of opacity in the data collection from start to finish. The black box here refers to the opacity of the decision-making process and the inability for the individual to understand what stems such a decision [30].

In other words, not reaching the transparency goal would mean that an individual giving personal data in order for the IoT device to give a solution would not be able to understand on what basis the decision was made and to obtain justifications on the reasons why this particular decision was given. This in mind, it is easy to see that the individual would find it hard to counter the decision as they wouldn't know nor understand the decision-making process. The decision could thus be made using prohibited criteria without the individual knowing [30].

7 Discussion and solution ideas

7.1 Unwanted surveillance

Throughout this paper, we have identified that the main problem about privacy protection comes hand in hand with unwanted surveillance. In fact, when looking at privacy infringement by household robots it is relatively coherent to focus on the surveillance such robots could exercise through their sensors such as their camera or microphone as it is thanks to those sensors that the surveillance of the individual can be performed. Hereafter the main aspects of such a surveillance will be discussed. First, the consent given to the surveillance will be examined, then, the different actors who are able to rely on unwanted surveillance in order to access information will be highlighted. Next, the attention will be directed towards self-censure and on the effects the surveillance has on the individual. Later, implications of data collection on children are discussed. Lastly, this paper will focus on the mechanical aspects of robots which can be used to maneuver that unwanted surveillance.

7.1.1 Consent

In this section, we will identify the rules of the GDPR that are in relation to the problem of consent. Indeed before we dig into the different actors able to exercise such a surveillance we must first understand, through the GDPR, how can an individual validly give free and informed consent. Are companies always obliged to gather the individual's consent in order to collect and use the individual's data ? Do companies always respect the rules of consent ? If yes, how ?

1. **GDPR**
   In general, according to the GDPR, consent has to be given in writing in order for the data to be collected (article 7 of the GDPR) [10]. In fact, consent cannot be presumed through silence or inactivity. However, in order for the consent to be correctly given and therefore for the company to be able to rely on the consent to gather the personal data, it has to be free and informed. Indeed, for the consent to be considered informed, the GDPR imposes to companies to provide a certain degree of information to the individual. These mandatory pieces of information are the following [31] [32] : ″

   - *Identity and contact information of the controller or his or her representative;*
   - *Contact information for the data protection officer, if there is one;*
   - *The collected data;*
   - *Processing purposes and legal basis;*
   - *Recipients of the personal data;*
   - *Possible transfer to a third country or an international organisation;*
   - *Retention duration or criteria for determining it;*
   - *Existence of the data subject's rights (access, rectification, deletion, limitation, opposition, portability + right to withdraw consent at any time);*

- *Existence of the right to lodge a complaint with the supervisory authority;*
- *Existence of automated decision-making."*

Once the individual was made aware of the information here-above, they will be able to give their consent. Therefore, for the company to correctly collect the individual's consent, the company will have to collect it in writing. For instance, the company could ask the individual to sign a form or, if online, to tick a box.

However, it is important to note that *"the person responsible for subsequent processing is exempted from the obligation to provide information when the provision of such information proves impossible or would require disproportionate efforts"* [32].

Moreover, if we look at the article 5 of the GDPR [10] we can see that the process of data has to be lawful and it meets that requirement through two different ways. The first one being that the individual or so called "data subject" has given consent. The second way is found through article 49 of the GDPR [10].

In fact, if one looks at the article 49 of the GDPR they will find situations in which, exceptionally, no consent has to be given for the collect of personal data to be considered lawful. those situations are the following [32] : *"*

- *The transfer is necessary for important reasons of public interest.*
- *The transfer is necessary for the establishment, exercise or defence of legal claims.*
- *Processing is necessary to respect a contract to which the data subject is party or to carry out pre-contractual measures at the request of the data subject.*
- *processing is necessary to fulfil a legal obligation to which the controller is subject.*
- *processing is necessary to safeguard the vital interests of the data subject or of another person.*
- *Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party."*

Now that the situations in which consent does not have to be given for the companies to collect the personal data of the individual have been pointed out, a few precisions on other rights linked to consent will be made.

Firstly, it seems important to remind the individual of its right to be forgotten. Indeed, under the article 17 of the GDPR [10], individuals will be able to ask for their personal data to be erased. However, this possibility will not be applicable in all situations. In this paper, it does not seem of importance to dig deeper into this subject as a lot of scientific work is already out there on this specific topic.

Secondly, the right to data portability will be examined. In other terms the individual should be able to receive his personal data which was collected and

have the right to transmit those data to another controller. In this regard, the article 20 of the GDPR [10] is very interesting. Some argued that it may be the first step in individuals selling their personal data. However, it does not seem to be reasonable to consider this outcome. In fact, if an individual wanted to sell its data, it would benefit from the legal basis of consent given in the article 6 of the GDPR. However, this article, as previously mentioned, provides with a mandatory provision which states that the consent has to be given for one or more specific purposes. Therefore, this wouldn't be considered as a sale as for a house to be sold for example, there is a real transfer of property. In the case of personal data, the company would have to specify the use made of the data in order to comply with the legislation. Moreover, as said hereabove, the article 17 of the GDPR provides with a possibility for the individual to see its personal data erased and for the consent to be taken back. These provisions therefore highlight the fact that a sale of personal data is to be considered quite uncertain in the near future [33].

2. **Users choices / privacy parameters**
   When talking about consent and transparency it is also interesting to talk about how it is going to be implemented in practice. What websites typically do when you enter them for the first time, is ask you to choose privacy settings. Especially regarding data collection and who would potentially gain access to that information. A similar feature could be implemented for household robots. And this type of personal information settings can already be found on devices such as Google Home or Amazon Alexa [34] for example.

   But the main problem is that they do not always explain clearly what type of information they collect and why they are collecting it for. If we take the average user of a website visiting for the first time, he will be welcomed by a pop-up telling him to configure his privacy settings. And those privacy settings are almost always set by default to share the maximum amount of information possible. And the interface is designed to make the user use those default settings and it does so by making it time-consuming to set the parameters to the minimum for the site to work properly and to maximize the privacy. The results of this design is that only a small fraction of people will actually bother to change those settings [35].

   All of these facts combined ensure the company that a large portion of its users will allow it to collect information about them. And in a sense it is only natural for them to do things that way because if we turn things around, and say that now by default almost no information can be used by big tech companies, users do not really have an incentive to activate the option to share their data other than to help improving the quality of the company's products.

   In the end, a good solution would probably be to force the user to go through the privacy settings when installing a device for the first time. Ideally the settings would also provide a short explanation of what data is collect and why it is being

used so that the user can make an informed decision about their choice instead of relying on default parameters set by the company. But then again, making a good interface that convey information about the robot intuitively is no easy task [36] and is really application dependant so standardizing the process might prove to be overcomplicated.

7.1.2 Different actors

In this section, we will examine the different actors who will possibly use the technique known as "unwanted surveillance".

7.1.2.1 Government

First and foremost, the government is the first actor who is more likely to utilise unwanted surveillance on individuals. In order to explain this phenomenon, the current sanitary situation seems appropriate. In fact, it was said that a few countries used such unwanted surveillance in order to better control the spread effect of the pandemic [37]. Majorly, the countries that used this surveillance are not part of the EU. For instance, Iran decided to use an app which was supposed to help people self-diagnose in order to get access to the individual's phone number as well as localisation. They managed to get such data from approximately 3.5 million people. As said previously, such a surveillance is mainly happening outside of the EU. However, Oxford University researchers presented to a few EU countries an app that would allow to follow the interactions between individuals. They believe that the current tracking of the virus is too slow. Another example is that of Belgium. In fact, Proximus, telenet and Orange will work together with Dalberg Data Insights in order to help the government. Once the belgian CNIL will have given its consent, they will create "mobility cards" which will utilise anonymised data and predict the evolution of the pandemic in that or that area (utilising the localisation of the individual). The GDPR does not prohibit the data collection without consent in case of a sanitary pandemic. However, the e-Privacy directive does not mention pandemics. This is why this utilisation is quite subject to interpretation [37].

Another example of the government utilising unwanted surveillance can be found when looking at the sanctions which were given to the European Parliament for violating the GDPR. In fact, the European Data Protection Supervisor took action against the European Parliament twice for not having protected the personal data of approximately 329 000 people [38]. In fact, the EDPS stated that the Parliament didn't ask for the permission needed to collect the data and stated that the Parliament didn't publish the confidentiality politic needed to use a website in time.

These are only a few examples amongst others. In fact, the EDPS inflicted around 114 million euros in fines since the coming into force of stricter confidentiality rules in mid 2018 [39].

7.1.2.2 Private actors

- **Manufacturers / Data controllers**
  Manufacturers of household robots and/or IoT devices, similarly to other companies operating in the digital world, have based their business models on the Big Data. Indeed, this massive amount of collected information allows to run machine learning algorithms, as well as to establish profiles. The device is thus able to predict the behavior of users and offer a personalized experience. This can lead to an unwanted surveillance if, among other things, the data controllers are collecting more data, and keeping them for a longer period, than what is needed (cf principle of privacy By Default from the art. 25 of the GDPR).

  This is the vision presented by Müller in [40] which argues that even though robots have not yet a central position in the data collection such as what is currently done by big companies through social medias or games, they are doomed to become part of the "data-gathering machinery" at their turn. In the article, the author talks about "surveillance economy" or "surveillance capitalism" to refer to this massive collection of data.

  In order to bypass the restrictions imposed by the GDPR relating to the use of personal data, manufacturers can use anonymization techniques. The concept is defined in the GDPR at the whereas (26)[9].
  In practice, a total anonymization of data is hardly achievable. Indeed, in [41], several anonymization techniques were reviewed and it led to the conclusion that some risks can remain, and that privacy protection depends on the engineering of those techniques.
  Alternatively, data controllers can pseudonymised their datasets, meaning that data *"can no longer be attributed to a specific data subject without the use of additional information"* (art. 4 (5), GDPR [10]). Pseudonimization of data as soon as possible would allow manufacturers to show their compliance with privacy by design and by default (whereas (78), GDPR [10]). Moreover, as stated by the whereas (156) of the GDPR [10], pseudonymization acts as a "safeguard", and offers wider possibilities to the data controller for the process of data, such as data processing *"for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes"*. Therefore, it should act as an incentive for the data controllers to pseudonymize the collected data.

  In [42], authors explain that, in the context of Big Data analytics, a person can be identified by the combination of non-personal data. Henceforth, pseudonymization or even anonymization could not be sufficient to protect individuals. An issue also arise from the opposite approaches used by the GDPR and the Big Data analytics. The former asks for a purpose in the treatement of data, while the latter consists of exploring large amount of data to detect trends without a

[9] *"The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable."* [10]

clear predefined purpose.
Among the challenges identified regarding the compliance of Big Data analytics with the GDPR, we can mention that the robustness of privacy-preserving techniques should be improved to be able to scale to accommodate the large amount of data without hurting the performance, as well as to deal with different types of data coming from various sources. This last point is essential since model accuracy is dependent on the diversity of data at disposal, but the sharing of data is not allowed in the current regulations.
The authors thus suggest 2 paths of solution in order to benefit from the sharing of data while preserving privacy. First, building trust between partners would allow to transfer data between those parties. Second, providing access to a secure environment with controlled protocols would allow data to stay in a single location where all parties could operate under the same privacy-preserving rules.

More precisely, various privacy-preserving technologies can provide solutions, which have been classified into 3 trends.
A first trend is changing the current paradigm about ownership of data to a user-centered data protection. In practice, this is materialized by the development of user-friendly interfaces featuring various parameters to exercise one's rights granted by the GDPR. On the controller side, the backend has to be adapted to accommodate those various actions (Right to be forgotten for instance). Blockcain technology can also be used to share sensitive data.
The second trend consists of designing automated processes to comply with the privacy obligations. To do so, regulations would have to be translated into a language understandable by a machine, which is hard to achieve and raises the discussion about whether hardcoding the laws is desirable or not.
The last trend, as already introduce earlier, relates to performing big data analytics *"in a privacy-friendly and confidential way"*. For this purpose, multi-party computation can be used. Instead of data being shared across different parties, it is encrypted or transformed analytics or analytics results that are shared to create a computational space acting as a trusted third party.

Those 3 trends offer an overview of the solutions available (some are still in their infancy) to manufacturer / data controller to comply with the GDPR regulation while still being able to exploit data to train algorithms. Tackling this issue is in the interest of manufacturers since implementing privacy-preserving technologies could give them a competitive advantage over their competitors [42].

- **Third-parties / Hackers**
  Hackers are malicious actors that could observe us either directly through the various cameras and sensors of our own household robots, or through the collection of personal data (for instance by sniffing the network).

  Back in 2009, the paper [43] carried out an exploratory research to shed light over security and privacy vulnerabilities encountered in household robots. This

paper is focused on the second option mentioned above, *i.e.* the illegal interception of personal data. It goes further by envisioning what could happen if the attacker were to take control of our devices.

Before collecting personal information, the hacker should detect the presence of the robot. The later can easily be remotely identified by intercepting and injecting packets, the robot being accessed through either its local network (wireless mode) or remotely over the Internet.
Then, the hacker can simply eavesdrop the data sent by the robot. He/she can thus catch the username and the password to access the robot, and can reconstitute the video from the intercepted packets, as demonstrated by the authors on robot WowWee Rovio.
Experimentally, the authors discovered that an attacker can take control of the robot using valid credentials. They mention that most of the risks identified can be mitigated simply with improved basic security and by using a secure wireless network. This is however not straightforward since it depends on the network configuration set by the user.

Different type of attacks can be envisioned. First, the robot could be used to damage objects within the house or to harm itself. Second, since surveillance robots are by definition turned on all the time, it is a entrypoint for the hacker to spy on the house and its inhabitants, especially since the video stream can be intercepted. Third, with the rise of robots for health care (eldercare, childcare, disabled care), those more vulnerable people could be injured. Finally, the robot controlled by an attacker could be used to psychologically harm the household.
On top of those threats, usage of several robots present in the house could enable the hacker to access complementary features. This last problem is more challenging since even though a robot could be individually designed to be safe, the combination of several robots can lead to severe vulnerabilities.

The authors argue that users of household robots may have wrong perceptions about the security level of those devices. To mitigate the aforementioned issues, either the design should be intuitive or metrics and other evaluation criteria should be developed. To this end, a list of questions is provided to help the reflection about security and privacy. It is also suggested that reviews and grades about the different appliances could be published to inform users. Already back in 2009, the authors advocated for a legal framework regarding household robots [43].

In [3], authors carried out a risk assessment regarding IoT-based smart homes. They identified various security threats among which the impersonation by intercepting credentials (as explained above), the injection of malicious code into the apps controlling the smart devices, the possibility of denial-of-service attacks, the access to a wide range of data, and the monitoring of people inside the house through cameras.
Possible means to mitigate the risks are using of biometric identifiers rather than

username-password credentials, securing networks and communication channels, appropriately configuring the devices, and getting aware of all those aforementioned threats.

7.2 Issues about self-censure

The possession of domestic robots equipped with AI can lead to several types of behavior on the part of the user. He may, first of all, feel suspicious of his robots. Indeed, some robots, such as those equipped with a camera, could, in the event of hacking, allow ill-intentioned people to collect images from the privacy and intimacy of users. A robot equipped with a microphone could record confidential conversations, for example we can think of the voice assistant Alexa, present in a connected speaker sold by Amazon. The company itself has recognized that this speaker records everything it hears to transmit everything to Amazon which will archive the audios and thus allow their analysis by employees [44].

These risks lead users to self-censor, to behave differently in the presence of a robot. Who among us has never felt uncomfortable in front of a surveillance camera? This self-censorship is comparable to what is called the "social cooling" phenomenon which reflects the generalized paranoia of a society which, in order to counter mass surveillance, prefers to cultivate it rather than to rebel against the exploitation of personal data. This phenomenon was denounced by the Dutch researcher Tijman Schep. The more data broking companies transform our innumerable digital traces (cookies, posted content, registration forms, etc.) into potentially harmful “derivative” data (sexual orientation, religious or political opinion, risky behavior, etc.), the more we live in an atmosphere of permanent suspicion [45].

To reassure users, the CNIL provides several precautions to be taken when dealing with intelligent robots :

- First, to be informed of the use of data by the manufacturer, the transmission of data to partners, the nature, even the identity of these partners, etc.
- Second, to be able to accept or refuse these operations (we refer to what was explained above regarding free and informed consent).
- Third, learn about the features of the device before purchasing, whether on sales sites or on discussion forums.
- Fourth, tailor your purchase to your actual needs (are the device connectivity features worth the extra cost and risk to my data?).
- Fifth, Check that we can disable physically (for example via a button on the device) or software (for example via the settings of the device) the Wi-Fi, the microphone or any other functionality that one not in use and that can be potentially intrusive [46].

The opposite behavior may also be observed : the friendly (sometimes human-like) appearance of household robots can influence the perception of its user and leads to the disclosure of sensitive information because the latter trust its device [47].

The user anthropomorphizes the robot, and can develop affection towards it. The robot is considered as a social actor by humans, and thus bonds are fostered in part because of its appearance as already said, but also because of it behavior, its facial expression that make it seems like understanding the user. He/she is therefore more likely to tell about his/her feelings, states of mind, secrets or any highly personal information, sometimes even more than if he/she was talking to an actual person. This is supported by the fact that users do not understand or even are not aware of which data is being collected and how. This is due to the novelty of robots entering the house [7].

In [7], privacy-by-design is suggested as a solution to protect user's privacy. However, taken alone, it is not sufficient because the users also shape their robots. Hence, the latter are responsible for their own privacy. To help them with the preservation of privacy, it is suggested that turning off the robot should be possible, and that a visible signal indicating that the robot is currently recording should be added by manufacturers to their products.

The third recommendation formulated above can be reiterated in this case. A counteraction is to raise awareness of users about the potential risks they could be exposed if they disclose sensitive personal data to their robot, which records the conversation. Initiating discussions, educating people, communicating about previous experiences are, among others, methods to make people aware of the privacy issues [7].

7.3 Data collection on children

The problem of unwarranted surveillance can arise from devices that are completely unsecure, resulting in a lack of privacy. Here, we are going to look at a case where unsecure device can harm minors. Let's illustrate this with the example of the doll "My Friend Cayla", an interactive toy that can communicates with children. It connects via Bluetooth to an application installed on a phone or tablet and when the kid talks to her, Cayla records what is said and converts the audio recording to text. The text is then transmitted over the Internet to a third-party database where it is used to search for answers, which is afterwards sent back to Cayla in order to answer the request. First of all, before talking about safety concerns, we have to ask ourselves if this doll, like any other smart robot used by children, is legally and ethically correct ? Is it acceptable for companies / foreigners to be able to collect data on children ? US consumer groups, as well as several EU bodies, had called for investigations of manufacturers because they believed the toy to be unethical and worried about the collection of data on children under thirteen [48].

Indeed, the collection of miner's data via this kind of connected toys causes several problems. First, a minor under the age of 13 cannot legally give consent. Indeed, to give consent, it is important to be over a certain age limit. Today, according to the provisions of the GDPR, the basic age limit is 16. On the other hand, the European reg-

ulation offers Member States the possibility of adjusting this limit between 13 and 16 years old. As an indication, the age of consent is 15 years old in Greece, the Czech Republic and Slovenia, compared to 14 years old in Italy, Austria, Cyprus and Bulgaria. It even goes down to 13 years old in Estonia, Denmark, Belgium, Ireland, Finland, Poland, Latvia, Spain, Portugal, United Kingdom and Sweden, in France the age of 15 years old has been retained. If a company therefore wishes to obtain the consent of the minor, it must obtain the consent of the person having "parental responsibility" [49]. This consent is however, as in the case of our doll, rarely requested from parents, not necessarily well informed of the fact that *"the company transfers conversation content to a service provider located outside the European Union"*, specifies the CNIL. [50]

Then the main problem is that the doll communicates with a phone without an encrypted protocol (i.e. bluetooth), which means that any device within a range of 10 to 15 meters can listen to what the child is saying and also talk with the child. It didn't take long for Germany's Federal Network Agency to realize the danger such a device could cause. Their statement about this device is as follows: *"There is a particular danger that toys are used as surveillance devices: anything the child says or other people's conversations can be recorded and transmitted to without the parents' knowledge. A company could also use the toy to advertise directly to the In addition, if the manufacturer did not sufficiently protect the wireless connection (such as Bluetooth), the toy can be used by anyone nearby to listen to undetected conversations"*. Controllers were able to observe that a person located outside, twenty meters away, could connect their cell phone to toys without having to identify themselves. In a February 2017 report by the BBC, a cybersecurity expert shows how Cayla is able to open a voice-activated door simply by having her repeat the code. Because yes, once logged in, anyone can make the doll say whatever they want, even insults, as shown in a video posted on Youtube [51].

Finally, in the event of hacking, the consequences can be disastrous, in 2015, an Internet user managed to recover the personal data of five million parents and 6 million young owners of connected toys. Among this personal information, pictures of children. This can lead to another legal problem, the publication of these photos on pedophile websites. The final decision was to ban the toy, at least in Germany [52]. In other countries such as Belgium, it is still possible to obtain the doll via the internet.

What are the possible solutions to protect children ? Educate parents. The CNIL advises several things:

- Be very vigilant regarding the connectivity possibilities offered by the toy, this implies to: check at least that the toy does not allow just anyone to connect to it, for example by checking that its pairing with a smartphone or on Internet requires a physical access button to the toy or the use of a password; change the default setting of the toy (password, PIN code, etc.); secure access to your smartphone and to your internet box with a password; secure access to the online account attached to the toy with a strong password different from your other accounts; check that the object has a light when it is listening or transmitting information on the Internet; inquire to verify that the toy does not present vulnerabilities

already known and easily accessible; perform regular security updates.

- Say as little as possible when registering: while the teddy bear or doll visually reassures parents, its sensors can still collect sensitive data such as photos or intimate conversations. Upon registration, communicate only the minimum information necessary for the service (for example, give a random date of birth if the system needs to determine an age); create a specific email address for the toys used by the child; use pseudonyms as much as possible instead of the name / first name; only activate the functions you really need.
- Disconnect the toy / erase the data: switch off the toy when it is not in use or to avoid capturing sensitive data; ensure the ability to access and delete data; turn off automatic sharing on social networks; erase its data on the toy and on the associated online service when it is no longer in use. [53]

7.4 Data analysis and recordings

7.4.1 Create personality profile of individual

Household robots can collect a large amount of data, including biometric data. Biometrics can legally be defined as the set of automated processes that enable the recognition of an individual based on the quantification of his or her characteristics, like :

- biological blood, saliva, urine, DNA
- morphological (fingerprints, finger shapes, face, etc.)
- behavioral (voice, keyboarding dynamics, gait, etc.)

These biometric data can be considered as sensitive data, they are data that provide information on political, religious, health, racial or ethnic origin, trade union life, sexual orientation, judicial history and so on (art. 9 RGPD) [29].

From a technical point of view, this information can be used to apply techniques based on the reduction of dimensionality, such as Principal Component Analysis (PCA), singular value decomposition (svd) or Probabilistic Matrix Factorization (PMF). The idea is to transform a set of variables that can be correlated into a set of new uncorrelated vectors. These new vectors are called principal components in the case of PCA. Since the main objective is to reduce dimensions, the original set of variables is larger than the final number of principal components. These techniques will make it possible to place an individual on a hyperplane whose dimension will be equal to n minus dimension reduction. The position of the individual on this hyperplane will be given by his biometric data. This operation could seem insignificant. However, if this manipulation is repeated on a whole population in order to project it on the same hyperplane. Each individual will find himself in the vicinity of other individuals forming groups g allowing to complete the missing information of the individuals based on the data of their group. This allows to retrieve more information about the individual than he can give.

Unlike any other personal data, biometric data is not attributed by a third party, nor even chosen by the person; it is produced by the body itself and designates it and no other, in an immutable manner. Unlike a password or an identifier, it cannot be modified. It is irrevocable.

The basic principle is that the processing of sensitive data is prohibited. In its recital 51, the GDPR explains that certain data are particularly sensitive from the point of view of fundamental rights and freedoms, so much so that they deserve specific protection because the context in which they are processed could give rise to significant risks to those rights and freedoms. There are exceptions to the processing of such information. Art. 9, §2 gives the cases in which the prohibition of processing does not apply : *"*

*a) The data subject has given his or her **explicit consent** to the processing of such personal data for one or more specific purposes, except where Union law or the law of the Member State provides that the prohibition referred to in paragraph 1 may not be lifted by the data subject.*

b) Processing is necessary for the purposes of fulfilling the obligations and exercising the rights specific to the controller or the data subject relating to employment law, social security and social protection [...]".

In order to be able to process sensitive data, it is therefore essential to be sure to be in one of the exception cases of art. 9, §2.

Let's take the example of our vacuum cleaner equipped with a camera or the Mr. Kitchen robot equipped with a hidden microphone: the vacuum cleaner can film our face or those of our loved ones and therefore collect biometric and sensitive data. The food processor can record our conversations and therefore also collect biometric or sensitive data. We must ask ourselves whether in these two examples the user was able to give his free and informed consent [29] before being able to use the devices. If so, the processing of sensitive data is therefore permitted.

The problem is that even in the case of consent to data processing, any misappropriation or misuse of such data thus poses substantial risks to the person from whom it originates: unjustified surveillance [29], hacking or usurpation of his or her identity for the purposes of fraud, even criminal, etc. [29]. Even a legitimate and well-supervised use in case of cyber-attack, compromise or error can lead to serious consequences. In this context, the issue of securing biometric data is essential and must be an overriding priority in the design of any project of this nature.

It is difficult to find an idyllic solution to this kind of problem. Indeed, this kind of data recovery is performed every day to improve the user experience of individual *i*. Whether it is to offer him a movie on TV, a video on his smartphone, or to buy this or that product because it is no longer in his fridge.

The storage of biometric data on an individual medium held by a user must always be preferred to centralized storage solutions in order to minimize the risks involved.

Only when absolutely necessary, in the absence of any alternative, can centralized storage be considered, subject to strict security measures.

7.4.2 Discussion on data collection by sensors

In this section we will focus our attention on sensors used in household robots (see section 3.2.1), more specifically on the most common ones and most sensible in regards to privacy.

- **Video camera**
  One of the most widespread sensors and whose generated data is at high risk of containing data that could infringe on privacy. Cameras are an important source of biometric data. They may also collect confidential data such as credit card banking information. Indeed, real-time object detection is an application of deep-learning, more precisely of an algorithm called YOLO [54]. YOLO is a state-of-the-art real-time object detection system that can detect more than 9000 categories of objects. This algorithm works on a convolutional neural network that allows to split each image into smaller boxes. (see figure 4).

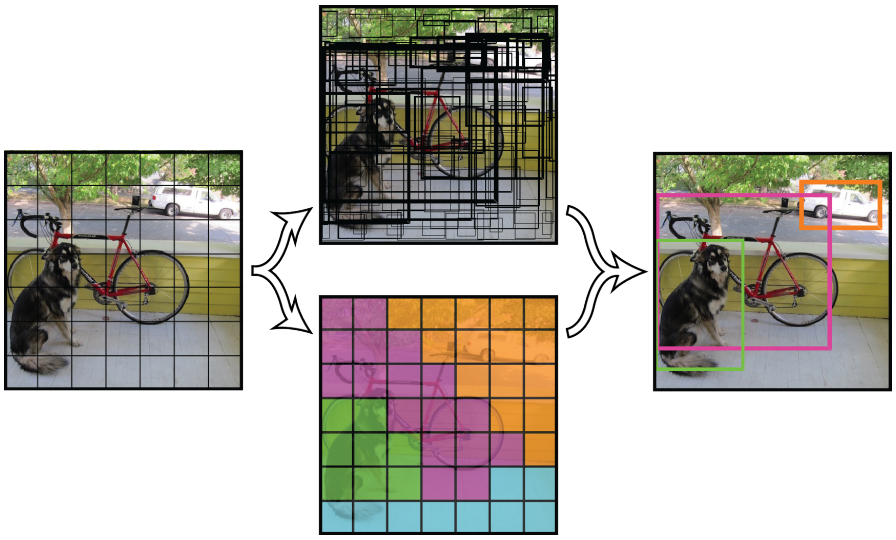

FIGURE 4: The Yolo system models the detection as a regression problem. It divides the image into a grid $S * S$ and predicts for each cell of the grid the bounding boxes B, the confidence for these boxes and the class probabilities C [54].

  Each box represents an area that must correspond to an object to be classified. This classification will then be done using Bayesian inference[10], which ensures the correct classification of the object. Note that the application of this kind of algorithm does not require a lot of power to operate and therefore any IoT device equipped with a camera is able to perform object detection in real time.

  These object detection methods can lead to an invasion of privacy but potential solutions to mitigate this effect exist. One possible solution [55] is to install

[10]Bayesian inference is a method of inference by which the probabilities of various hypothetical causes are calculated from the observation of known events. It is mainly based on the Bayesian theorem

filters to alter the images produced by the camera. The goal of the filters is to protect the privacy of the user while still allow for good performance of the robot. An example could be to blur the image enough so that text can no longer be read but shapes can still be recognised. That would mean that what is written on our credit card can not be read from the camera inside the household robot but that the robot could still be able to identify the credit card as a rectangular shape. What we get in the end is a trade-off between privacy and performance. The positioning of the user regarding this trade-off could be made by the user himself, giving him more control over his device and privacy.

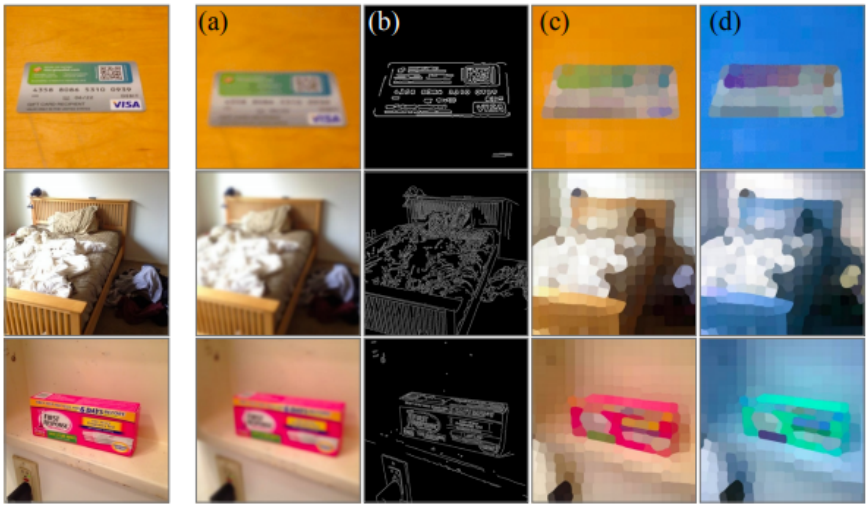

FIGURE 5: Examples of possible filter [55]

- **Microphone**
  Just like a camera, a microphone is capable of gathering a lot of information. Indeed, although its main use is to record, it can also emit. A microphone is also able to record a moment without noise and deduce by Bayesian inference a lot of information. For example, the fact of not recording noise knowing that it is dark allows to infer with a high probability that you are either sleeping or that you are not at home. Combined with a tracking of your position, it is easy to answer this question. By repeating this procedure, we understand that it is relatively easy to identify your routines. By following this same analogy, it is possible to identify the time of day when you have lunch and listen to the sounds at that time and for example to identify the type of coffee machine you own (bean, brewer, backsplash etc). This could potentially allow to better target advertisements that you are more likely to be sensitive to.

  In addition to what was mentioned before, a microphone is also a source of biometric data as voice can be used to authenticate an individual [56]. This fact alone should be of significant importance when talking about sharing that information and the moral and security issues that comes with it. But there is something even more concerning, it is possible to *"imitate a new speaker's voice using only a small amount of speech sample"* [57]. This means that by having

access to a device that contains or enables to retrieve voice recordings (like an Alexa or a Google home) it would be possible for someone to imitate the voice of the user of the device. This could lead to some very serious case of identity theft, as it could be done remotely and relatively easily.

- **Other data sources and the potential of inference**
  There are a lot of ways to gather data about the surrounding environment (see `section` 3.2.1) and even more different types of data to be collected. This means that it is possible to record many different phenomena inside a house and potentially also automate many of them. You could monitor the electricity consumption, the ambient temperature and so on. One important thing to consider is that the more information you gather the more information can be inferred. For example, if you have a smart thermostat that regulate heating for your home, smart locks for your doors and a charging station for your electric vehicle. All of these devices individually can not accurately tell whether you are at home or not but once you combine all of their data you can predict with much more confidence whether someone is at home or not. So connecting all your devices on a same interface and/or storing all of their information together can be quite powerful but as such must be treated with caution. A good practice is to ensure that all of that information is safe and not easily accessible just for the sake of convenience.

7.5 Solution idea for data storage

One of the solutions to this massive data collection is to give back the ownership of the data to the owner. The main solution explored by some governments and specialists is the concept of data pod. In few word, a data pod helps you gather, store, manage, use and share your data. It provides you with tools to control what information you share with which people and which organisations. In other word, a data pod is a personally owned database that permit you to be in control of your data, instead of the big companies like it is the case nowadays. You can think of a world where the government provides you a database at birth and all your personal data will only be stored on this database, and when a big company want to use your data, they will need to ask for permission to access a portion of your personal database. Therefore with this infrastructure, the management of the personal data is given back to the owner. This idea is currently being developed at MIT with the Solid project [58].

8 Conclusion

Throughout this paper, an overview of important technical aspects which are needed to understand what is a household robot, how it collects data and why, as well as a legal discussion regarding privacy, consent and unjustified surveillance was given and explained.
To conclude, it seems important to repeat that in order for a customer to trust the robot and its artificial intelligence, it should be aware of what type of data is collected and how it is processed. Transparency about how the robot works is a key element to build trust in the machine. It is only thanks to this information that the customer will be able to consent validly to the use of its data.
The main take-home message is that a trade-off is to be found between the collection of data and the respect of privacy of each individual. And while the European Union has already taken great steps with regards to the privacy of its citizens, it should still be actively working with specialists to determine what regulations would better protect its citizens while continuing to drive innovation.

Bibliography

[1] HLEG. A definition of AI : main capabilities and scientific disciplines. Technical report, European Commission, Brussels, dec 2018.

[2] Keyur K Patel and Sunil M Patel. Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges. *International Journal of Engineering Science and Computing*, 6(5):6122–6131, may 2016.

[3] Bako Ali and Ali Ismail Awad. Cyber and physical security vulnerability assessment for iot-based smart homes. *Sensors*, 18(3), mar 2018.

[4] Pierre Geurts and Louis Wehenkel. An introduction to machine learning. In *Cours Introduction to Machine Learning*. University of Liège, 2020.

[5] Rodolphe Gelin. *The Domestic Robot: Ethical and Technical Concerns*, pages 207–216. Springer International Publishing, Cham, 2017.

[6] Rafael Mateo Ferrús and Manuel Domínguez Somonte. Design in robotics based in the voice of the customer of household robots. *Robotics and Autonomous Systems*, 79:99 – 107, 2016.

[7] Christoph Lutz, Maren Schöttler, and Christian Pieter Hoffmann. The privacy implications of social robots: Scoping review and expert interviews. *Mobile Media & Communication*, 7(3):412–434, sep 2019.

[8] Leah Pickett. Voice Controlled-Appliances, Robots: Enter the Smart Home. *Appliance Design*, 66(4):12–14, apr 2018.

[9] Cambridge University Press. *Data : meaning in the Cambridge English Dictionary*, Accessed December 10, 2020. Link.

[10] European Parliament. *General Data Protection Regulation*, Accessed December 10, 2020. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, Link.

[11] European Commission. White paper on artificial intelligence: a european approach to excellence and trust. White Paper COM(2020) 65 final, European Commission, Brussels, feb 2020.

[12] Merriam-Webster Dictionary. *Sensor*, Accessed December 10, 2020. Link.

[13] Jim Tully Peter Middleton, Peter Kjeldsen. *Forecast: The Internet of Things, Worldwide, 2013*, Published November 18, 2013.

[14] HP Company. *HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack*, Published July 29, 2014 and accessed December 10, 2020. Link.

[15] Eric Zeng, Shrirang Mare, and Franziska Roesner. End user security and privacy concerns with smart homes. In *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*, pages 65–80, 2017.

[16] Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. Privacy expectations and preferences in an iot world. In *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*, pages 399–412, 2017.

[17] M. Frustaci, P. Pace, and G. Aloi. Securing the iot world: Issues and perspectives. In *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*, pages 246–251, 2017.

[18] Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J. Alex Halderman, Luca Invernizzi, Michalis Kallitsis, Deepak Kumar, Chaz Lever, Zane Ma, Joshua Mason, Damian Menscher, Chad Seaman, Nick Sullivan, Kurt Thomas, and Yi Zhou. Understanding the mirai botnet. In *26th USENIX Security Symposium (USENIX Security 17)*, pages 1093–1110, Vancouver, BC, August 2017. USENIX Association.

[19] Cloudflare. *What is a DDoS Attack?*, Accessed December 10, 2020. Link.

[20] Directive ni. directive (eu) 2016/1148 of the european parliament and of the council of 6 july 2016 concerning measures for a high common level of security of network and information systems across the union.

[21] John A. Foulks. German it security law. *Journal of Law & Cyber Warfare*, 6(2):165–190, 2018.

[22] Alan Butler. Products liability and the internet of (insecure) things: Should manufacturers be liable for damage caused by hacked devices? *50 U. Mich. J. L. Reform 913 (2017)*, 2017.

[23] European Commission. *Ethics guidelines for trustworthy AI*, Last updated on 17 November 2020 and accessed December 10, 2020. Link.

[24] X., *RGPD et Intelligence Artificielle : quel(s) impact(s) mutuel(s)?* Available on www.orange-business.com. , 2019. Link.

[25] Calo, Ryan, *Robots and Privacy* (April 2, 2010). ROBOT ETHICS: THE ETHICAL AND SOCIAL IMPLICATIONS OF ROBOTICS, Patrick Lin, George Bekey, and Keith Abney, eds., Cambridge: MIT Press, Forthcoming, Available at SSRN: https://ssrn.com/abstract=1599189.

[26] European Parliament. *General Data Protection Regulation, Art 25*, Accessed December 10, 2020. Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, Link.

[27] Information Commissioner's Office (ICO). *Data protection by design and default*, Accessed December 10, 2020. Link.

[28] Le Parisien. *Le «Monsieur Cuisine Connect» de Lidl contient-il un micro espion ?*, Published June 13, 2019 and accessed December 10, 2020. Link.

[29] F.COUDERT, C.GAYREL. Cours de droit de la protection des données personnelles, 2020, Ulg .

[30] Alexandre De Streel, Adrien Bibal, Benoit Frenay, and Michael Lognoul. *Explaining the Black Box: when Law Controls AI*. CERRE, 2020.

[31] Union Européenne. *Protection des données et respect de la vie privée en ligne*, Accessed December 10, 2020. Link.

[32] UCLouvain. *RGPD (Règlement Général de Protection des Données)*, Accessed December 10, 2020. Link.

[33] calimaq. *Le RGPD interdit-il aux individus de « vendre » leurs données personnelles ?*, Published May 12, 2018 and accessed December 10, 2020. Link.

[34] Amazon. *Manage Your Alexa Privacy Settings*, Accessed December 9, 2020. Link.

[35] Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. Dark patterns after the gdpr: Scraping consent pop-ups and demonstrating their influence. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, Apr 2020.

[36] Na Lin, Tong Shen, and Chaoyi Zhao. The usability of interactive interfaces design of intelligent household appliances: Take smart sweeping robots as an example. In Tareq Ahram and Christianne Falcão, editors, *Advances in Usability and User Experience*, pages 291–301, Cham, 2020. Springer International Publishing.

[37] Raphaël Balenieri. *Coronavirus : quand les Etats font pression pour utiliser les données personnelles*, Published Mars 18, 2020 and accessed December 10, 2020. Link.

[38] Alice Vitard. *Quand le Parlement européen est sanctionné pour la violation du RGPD*, Published December 2, 2019 and accessed December 10, 2020. Link.

[39] Stéphane le calme. *Bilan du RGPD : les régulateurs européens ont infligé plus de 114 millions d'euros d'amendes*, Published January 20, 2020 and accessed December 10, 2020. Link.

[40] Vincent C. Müller. Ethics of Artificial Intelligence and Robotics. In Edward N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, winter 2020 edition, 2020.

[41] European Commission. *Opinion 05/2014 on Anonymisation Techniques*, Adopted on 10 April 2014. This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC. Link.

[42] Data protection in the era of artificial intelligence. Trends, existing solutions and recommendations for privacy-preserving technologies. Technical report, BDVA, oct 2019.

[43] Tamara Denning, Cynthia Matuszek, Karl Koscher, Joshua R Smith, and Tadayoshi Kohno. A spotlight on security and privacy risks with future household robots. In *Proceedings of the 11th international conference on Ubiquitous computing*, Ubicomp '09: The 11th International Conference on Ubiquitous Computing, pages 105–114. ACM, 2009.

[44] X., *Alexa : Comment Amazon analyse votre vie privée*, available on www.lecafedugeek.fr. , 2019. Link.

[45] L.Encinas,"*Le social cooling, symptôme numérique de la surveillance de masse*", available on www.ubseketrica.com. , 2018. Link.

[46] CNIL, "*Robots connectés et données personnelles, conseils de la CNIL*", available on www.cnil.fr. , 2019. Link.

[47] Kaori Ishii. Comparative legal study on privacy and personal data protection for robots equipped with artificial intelligence: looking at functional and technological aspects. *AI and Society*, 34(3):509–533, sep 2019.

[48] The Electronic Privacy Information Center and The Campaign for a Commercial Free Childhood and The Center for Digital Democracy and Consumers Union. Epic ipr ftc genesis complaint, 2016.

[49] S.Meunier. *Les règles du RGPD concernant le consentement des mineurs sont-elles efficaces ?* available on www.itgovernance.eu, 2018.

[50] L.Ronfaut. *Sécurité : la Cnil accuse deux jouets connectés d'atteinte grave à la vie privée des enfants* available on www.lefigaro.fr, 2017.

[51] T.Schonheere. *Cayla et I-Que, les jouets qui peuvent (toujours) espionner vos enfants*, available on www.franceinter.fr, 2017.

[52] Germany's Federal Network Agency. Bundesnetzagentur removes children's doll cayla from the market, 2017.

[53] CNIL. *Jouets connectés : quels conseils pour les sécuriser ?*, available on www.cnil.fr, 2019.

[54] Joseph Redmon and Ali Farhadi. *YOLO9000: Better, Faster, Stronger*, 2016. cite arxiv:1612.08242.

[55] D. J. Butler, J. Huang, F. Roesner, and M. Cakmak. The privacy-utility tradeoff for remotely teleoperated robots. In *2015 10th ACM/IEEE International Conference on Human-Robot Interaction (HRI)*, pages 27–34, 2015.

[56] A. Shoup, Tanya Talkar, and J. Chen. An overview and analysis of voice authentication methods. 2016.

[57] Younggun Lee, Taesu Kim, and Soo-Young Lee. Voice imitating text-to-speech neural networks, 2018.

[58] MIT. *Solid Project*, 2016 - present. Link.