# From the Glass House to the Hive: The Private Sphere in the Era of Intelligent Home Assistant Robots

Silvia Conca



# From the glass house to the hive: the private sphere in the era of intelligent home assistant robots

Silvia De Conca[1][0000-0002-9356-9815]

[1] Tilburg Institute for Law, Technology, and Society (TILT), 5000LE Tilburg, The Netherlands
s.deconca@tilburguniversity.edu

**Abstract.** This paper introduces a re-conceptualization of the private sphere, following the presence inside the house of intelligent personal assistant robots that observe and act through sensors and actuators, and aggregate the data collected in the Cloud. This processing inserts the personal sphere of individuals into a complex and multi-layered informational structure, a "hive" of private spheres. An abstract model, named Aggregated Privateness Model, is presented herein to explain the dynamics of the "hive". It sheds new light on a more collective dimension of 'private', a dimension which represents a context by itself, with normative mathematical rules and in which the expectations of privacy of individuals can be infringed based on the uses made of aggregated data. The Model also highlights how the behaviour of the individuals can influence the other private spheres in the cluster, as well as the Aggregation itself, due to a network effect, and how Diffused Network Liability could help compensating for such influences without incurring into practical impossibility.

**Keywords:** Privacy · Robotics · Artificial Intelligence · Big data.

## 1. Introduction

Small, sleek, minimal speakers, designed to be put on a desk or on the living room table. Bigger gadgets, with monitors showing a simple smiling face that follows with its 'eyes' the human while it moves around the room. Or else, little apparatuses with wheels and small arm-like tools, that can stroll with the human around the house while answering their requests. All around them, a multitude of connected 'smart' devices: thermostats, video/photo cameras, televisions, refrigerators, light switches, door locks, ear plugs, even wardrobe assistants. The products described above form a new family, identified in the rest of this paper as intelligent personal assistant robots, and are designed to help consumers during their daily lives by organising and coordinating tasks around the house controlling the smart devices connected to them. In this paper, I will argue how these small devices bring with them an important effect for our private spheres. The potential for surveillance and hacking of these devices has already caught the attention of the public and scholars. The focus of this paper will, however, be on how the presence of such intelligent devices (virtually) moves the house within a dense structure made of the information harvested from the private spheres of individuals,

aggregated and combined to create patterns and profiles. Their unique combination of sensors, actuators, the central brain of the devices and their use of Internet and Cloud computing creates a fundamental change *inside* the most sacred space of protection of the private sphere: the house.

It is this concurrence of elements (the intelligent personal assistant robots, their features, their contribution to Big Data, their presence inside the house) that makes this analysis meaningful and necessary. This paper contributes to the general discussion concerning privacy by proposing a Model to visualise and analyse the modalities with which the presence of such a new and permeating technology provokes changes in the relationship between the private sphere and the house. The Aggregated Privateness Model, as explained below, highlights new features for the private sphere, showing a shift from the individual to a more collective dimension of "privateness".

The scope of the analysis and the Model proposed is, however, far-reaching and goes beyond the specific case of intelligent personal assistant robots.

These robots stand at the crossroad of different industries, whose technologies build on each other: Internet of Things, Ambient Intelligence, Artificial Intelligence, and Big Data are only some of the elements combining into them and, as a consequence, into our houses. For this reason, while the starting point of this paper are intelligent personal assistant robots, the story it tells stretches to other domains too. While the starting point of the analysis was given by intelligent personal assistant robots, the Model has a broader scope, and can help analyse the effects on the private sphere of other technologies and industries too. It should be seen as a framework within which different stories can find their places, based on the technology, or technologies, it is applied to.

The first part of the paper sets the stage for the analysis, presenting the changes undergone by the house due to the introduction of new technologies. The features of intelligent personal assistant robots are also discussed, with a focus on their influences on the traditional construction of the private sphere. The first part is completed by an overview of what aggregation means based on how the data collected inside the house by the intelligent personal assistant robots are mined and processed with machine learning. The second part of the paper introduces a change of perspective. Tracing a line between the aggregation of data and the subsequent aggregation of the private spheres of the individuals to which those data belong, it culminates with the introduction and explanation of the Aggregated Privateness Model. This latter, inspired by the structure of snowflakes, provides for a conceptual framework to explain the main changes occurring in the private sphere: the introduction of a new context for individual perception of "privateness"[1], at aggregated level, and the capability for the individuals associated with a profile to influence, changing also how it will be applied to others. Finally, in the Conclusions the Aggregated Privateness Model is inserted into a broader context, with a brief explanation of its potential applications to privacy and personal data protection, for possible future developments of the analysis.

[1] The use of the word privateness is here preferred over the word privacy. While, in fact, this latter retains a meaning strictly connected to the legal protection of the private sphere, the word privateness is meant to embed the idea of the very essence of the private dimension of individuals, regardless of its content, protection or of the legal status connected to it.

### 1.1. The Haunted House

In the last decades, we have witnessed a significant change in the way houses are equipped. Electronic and digital devices are becoming ordinary appliances, and the tendency shown by producers and designers is to integrate more and more a wide range of digital apparatuses into the domestic environment. So far, most of such devices were controlled one by one by the owners directly, through their mobile phones or computers. With the entrance in the market of intelligent personal assistant robots however, the coordination among the different sensors and devices can be carried out not directly by the owners, but by their assistant robots, whose main purpose is to organize and simplify the lives of those living inside the household environment.

Two prominent examples of intelligent personal assistant robots are Amazon Echo[1] and the newly presented Google Home[2]. Both Echo and Home do not possess kinetic capabilities. They consist of minimal design speakers, which can be activated via a trigger word or buttons. Rosie, the Jetsons' humanoid robot with wheels and arms carrying out chores around the house is replaced by decorative desk units run by software that interact with the owners through voice command ("Alexa, play the playlist named …", or "OK Google, increase the room temperature to…")[1][2]. They do not present arms or other actuators, and the number of sensors directly embedded on the devices is very limited. To complete tasks they deploy other devices connected to them, such as a speaker or thermostat, in order to both collect the information necessary to elaborate a strategy, and then act following it.

Another significant feature of most intelligent personal assistant robots is given by the fact that while their functions necessitate huge amounts of data, they are not equipped with proportional storage hardware. Intelligent assistant robots transfer all the information they collect on Cloud, where they are stored for future use. In the Cloud, the information is also elaborated, in order to carry out the tasks requested by the owners. In the case of Echo, for example, logs of the voice commands are stored in the Cloud and processed to, among others, improve the robot's natural language recognition skills, in order to minimize errors for future requests by the owners. For this reason, the deletion of part or all the logs can give as a result a less efficient performance of the Echo.

Intelligent personal assistant robots coordinate the sensors and actuators, functioning as a central brain, with a certain degree of autonomy that builds upon machine learning and the deepening of the knowledge of their owners. Those are also the features distinguishing home-located personal assistant robots from simple smart phones, from which individuals can activate devices inside the household environment by means of special apps that, however, do not coordinate and do not operate in autonomy, serving as mere 'remote controls'.

Google Home, Amazon Echo, and other similar devices stand on the verge of several different technologies: Internet of Things, Ambient Intelligence, Artificial Intelligence, Robotics, Computing. Intelligent personal assistant robots present an additional element differentiating them from other similar technologies, such as Internet of Things

or Ambient Intelligence: their proactivity, which also represents an important component of their intelligence. While acting as the central brain that coordinates all the other smart devices, intelligent personal assistant robots adapt their internal parameters thanks to their own self-learning algorithms. Even though they (mostly) follow the vocal commands of their owners, the decisions about how to accomplish their tasks are taken autonomously, based on what the robots have learned from the data collected around the house. In certain cases, the robots might prove even too much proactive, unexpectedly accomplishing tasks or providing for information unsolicited[2]. For these reasons, these devices are identified in this paper as robots, and not as mere "smart" speakers [3].

The embedding of connected devices and intelligent assistant robots inside the house, with the constant scanning for information and their subsequent transfer and elaboration, represents a powerful moment of evolution for the role traditionally assigned to the home in the protection of the private sphere.

The boundaries between the public and private sphere have been moving around the threshold of the house during the centuries[4][5], sometimes pushed towards the inside of the household environment, sometimes lingering around the doorstep, and other times pulling towards the outside of the house. In the Western tradition, the house is considered the *fulcrum* of the private life: the place where individuals and families can hide from the sight of the community or the State, fully expressing their inner selves while carrying out their personal and intimate activities. In other words, the house is considered as the physical place where the private sphere could be protected from undesired interferences, and therefore find its full expression and expansion[6]. The private sphere, however, has not been unanimously and neatly defined. Its definition changes based on the time and culture, as well as on the tension between its conceptual opposite, the public sphere. For this reason, this paper uses as a starting point a functional definition of private sphere, consisting of the range of behaviors and knowledge, whose disclosure individuals desire to avoid (or at least limit) regardless of the addressee (other individuals, public or private entities). The increased availability and interconnectivity of smart consumer products destined to be placed inside the house, however, is often seen as a threat to the functions of seclusion and isolation provided by the house, whose (political) role is influenced by the economy-dictated values of home appliances, in what has been defined as a "democracy of the microwave" [7] (or, in our case, of the smart microwave).

Literary images such as Bentham's Panopticon, Orwell's Telescreens, or Zamyatin's glass houses are often evoked to describe the new vulnerability of the private sphere caused by the digitalization of home appliances. Cases like the one happened in Arkansas, in the United Stated contribute fueling those concerns. In a murder trial, in fact, an

[2] As occurred with thousands Google Home Mini distributed during their launching even in the October 2016. In the following weeks, it was discovered that a fault in the products had made them activate up to over a thousand times a day, recording almost entire days of their users. The fault appeared to be an overly sensitive sensor that activated following the vibrations generated by a wide range of random sounds.

Amazon Echo sat on the witness bench, and its logs have been requested with an affidavit by the public prosecutor as evidences against the Echo's owner. In such cases it is, however, possible to also have a glimpse of other mechanisms and aspects connected to the introduction of intelligent robotic devices inside the house. In the abovementioned murder trial case, for instance, Amazon's lawyers in a first moment challenged the request for the device's logs, claiming that both the recordings of the user/defendant's voice and the replies of Alexa (the software managing the device) fell within the protection of Freedom of Expression. While the recordings of the voice of the subjects were indeed directly protected under the First Amendment, Amazon's position is that the replies and tasks of Alexa, being tailored on the personality of the owner based on the data collected over time by the device, were also, indirectly, representing his forms of expression, as well as the forms of expression of the company's software and databases, Amazon Inc.[8]. It is in these, apparently minor, arguments that the issues connected to surveillance leave the stage to the issues deriving from the processing of the information made by the intelligent assistant robot starting from the private sphere of the individual, to how the processing affects the individual regardless of State intrusions.

While the first concerns are indeed justified and important, the focus of this paper will not be on surveillance, but on the complexity of the circulation of data within and around the house, switching the perspective from the eyes glazing from the outside, to the relationship between those complex interactions and the 'interior' of individuals' private spheres.

The issues raised by intelligent robotics in the home offer us the chance to change the perspective. While, in fact, anonymization and encryption techniques still contribute to the protection of the private sphere and to maintain the threshold (even if with some blurring sections) between public and private, the fluxes of data exiting and entering the house can shed a light on the structure in which the private sphere is inserted, a structure that highly depends on machine learning technology and fuels the hunger for data which characterises the Information Society. The protection of the private dimension of individuals must, therefore, not only consider the risks posed by invasive technologies, but also individual's behaviours and preferences in terms of consumer products and services, as well as the environment in which personal data are inserted.

While, in fact, new and updated provisions of law try to keep up with the technological progress, their concrete application might still rely heavily on judicial decisions. Ambiguous, industry-neutral provisions require years before a consolidated line of action is formed. For this reason, the paper proposes an approach that, notwithstanding its abstract nature, can provide for a much-needed uniform, conceptual basis, to avoid distortions and damages to individuals to occur while the law consolidates the lines of its implementation.

Before proceeding with the analysis, however, it is necessary to understand what do machine learning techniques and the Big Data phenomenon imply for the life cycle of personal data collected by intelligent personal assistant robots and for their elaboration. For this reason, the following paragraph will explain the fluxes in which information

exit and enter the house, and will introduce the basis of the Model proposed in this paper: aggregated data.

### 1.2. Aggregated Data

Intelligent assistant robots collect information and data from the environment surrounding them via several sets of sensors: audio, video, movement, temperature, humidity, and so on.

Once in the virtual 'prairies' of the Internet the information collected from the private spheres of individuals are the object of different kinds of machine learning operations, aiming at creating categories of subjects, preferences, or behaviors.

Using mathematical rules (such as association, probabilistic, regressive rules), machine learning is capable of analyzing values, weighing them based on the data available, identifying direct or indirect influences among the quantitative or qualitative elements available. In this way recurring elements, or patterns, are highlighted that allow for categorizations and mapping of the behaviors of the subjects presenting similar characteristics.

The results of the processing of the information and data collected inside the private sphere are multiple. The most evident one is indeed the creation of profiles or models, either containing a projected description of a specific subject or, on the opposite, hypothetical and statistical representations. Both kinds of profiles are divided by Vedder[9] between distributive and non-distributive, meaning that the features of the profile respectively all apply to all the individuals or, on the contrary, do not all apply to each and every individual falling within such profile[10]. Since every profile relates to a specific purpose (marketing for different products or services, rating for financial institutions, medical services, criminal activities, etc.), individual information is elaborated to harvest a wide range of results, which translate into a wide range of profiles all being added, layer after layer, on top of the same subject.

Models/profiles also bring with them less obvious results. The main one is that flexibility and uncertainty are an intrinsic part of the elaboration. The models consist of correlations that go beyond the causal connection. The concrete accuracy of such predictions is, however not guaranteed, due to the many variables involved, and to approximation. Uncertainty is an intrinsic feature of profiling. A certain degree of flexibility is also often included in the system. Flexibility derives from the relationship between the descriptive assumptions (such as: "women age 18-40 are prone to online clothing shopping") and the numbers capable of statistically support such description (the percentages of online clothing shopping performed by women in that age range).

The profiles added on the subjects are not, therefore, immutable, but change based on the variations of the variables processed. The creation of models containing new and additional derived information, their juxtaposition over the individuals, and the uncertainty and flexibility embedded in them, as well as the introduction of information derived from background knowledge or from other sources, all contribute to the creation of additional layers on top of the individual[11]. Aggregated data are the product of the interdependency of information coming from the private sphere of different individuals. The final result of such clusters of data is eventually re-inserted among the data of

the single subjects in an operation that might, or might not, correspond to the will and desires of the person profiled.

Aggregated data can be found distributed in the multi layered structure of profiles that is juxtaposed to the individual sphere; they do not match the original data harvested around the individual, but they can, in part or in full, create an image that matches the one of the subject while, at the same time, connecting this latter to the images of the others included in the same profile.

To better exemplify the creation of the additional layers of profiles on the individual, consider the previous example of online purchases of women between 18 and 40. A first layer added on the individual is the one concerning the preference for online clothing shopping. In addition to that, another layer is given by the preferences for yoga attire over, for instance, volleyball clothes, based on the proximity or not to the address of a subject of a yoga center and on the information deriving from the credit card with which the subscription to the yoga classes was paid. Further processing might reveal additional patterns, such as the preference for neutral colors based on age ranges and professions. Other profiles and, therefore, further layers are added. The data concerning the thermostat and temperature preferences, as well as the geographical location of the subject, can also imply preferences in terms of entertainment, leading to the inclusion of the subject within the group of people that, for instance, prefers to stay in and purchase on demand movies or subscription to services such as Netflix. This additional layer, in turn, can provide insight over snack and alcohol consumption, and so on.

## 2. Proposing a new approach

**From the aggregated data to the aggregated private spheres.** The aggregation of data creates a 'hive', an informational structure composed of profiles and categories, the result of data mining and processing of information coming from different subjects. Once individuals are associated with certain profiles based on - and as a consequence of - the information harvested from them, their private sphere can be seen as annexed to the informational structure.

Figures 1 and 2 below show how profiles overlap on top of an individual. Figure 1 shows the result of mapping the musical preferences of an individual A. Based on the songs listened to by A on Spotify, crossed with the information concerning the classification of songs into different genres, and on the genres preferred by other individuals on Spotify belonging to the same age group and geographical location of A, a certain musical profile of A is created. Such profile is then used to suggest A new songs and bands. The processing and mining of A's data, as well as of the data of other subjects, led to the aggregation of their private spheres (consisting of the behaviors and tastes concerning music) into clusters based on age, gender, geographical location, and other features.

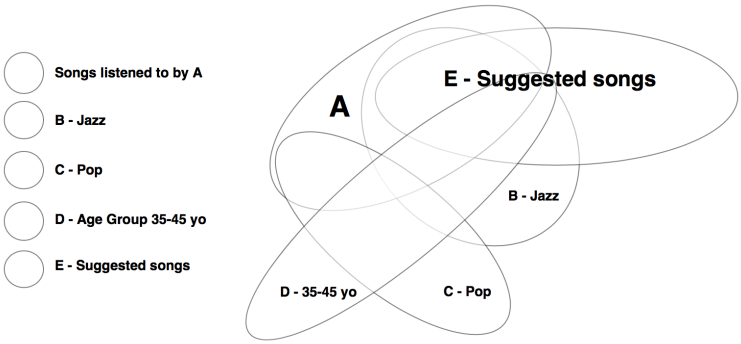


**Fig. 1.** The model created based on the data concerning musical tastes of A, the genres associated to songs, the Age Group A belongs to, and other songs listened to by subjects with similar age.

In Figure 2, the aggregation leads to the insertion of the private sphere of A into another cluster: based on A's preference for jazz and on the age-group A belongs to, A's profile is associated with higher wine consumption (over liquors like vodka or tequila). Also in this case, A's private sphere is intertwined with the private spheres of all the other subjects whose data are used to identify the models, forming an information structure with them.

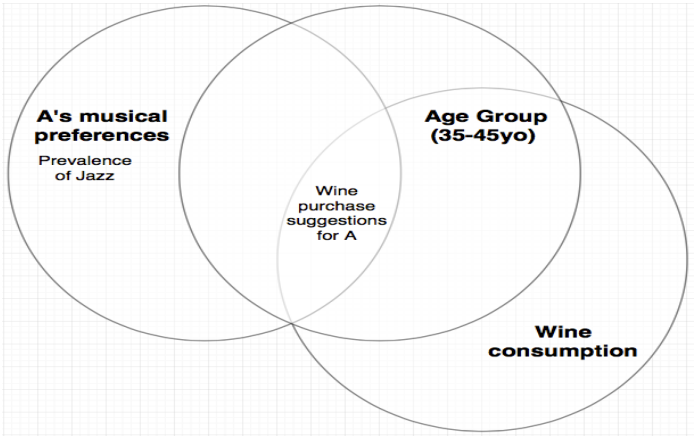


**Fig. 2.** The model created based on the data concerning musical tastes of A, the Age Group A belongs to, and habits of alcohol consumption of subjects with similar musical tastes and age.

As illustrated by Figures 1 and 2 above, the circumstance that the profiles are created based on multiple individuals' preferences embeds the private spheres of those individuals, creating links among them. In this way, clusters or aggregations are created, some

of which are connected or overlapping with others. This set of clusters and aggregations is what is here indicated, in abstract terms, as an informational structure.

The main features of the informational structure are dictated by the very nature of the technology involved, as described above: machine learning collecting information from within the house, coordinated by the assistant robot's central brain, processing them based on algorithmic models, and returning them to the individuals in the form of tasks performed inside (and sometimes outside) the private sphere. Based on how the aggregation of data works, it is possible to identify three main characteristics of the informational structure: the presence of flexibility and uncertainty within the structure, influences deriving from network mechanisms within the structure, and a dichotomy between transparency and opacity. Such elements can have significant consequences on the way intelligent assistant robots in the house affect the private sphere.

In order to analyze the features and effects of the insertion of the private sphere inside the informational structure a conceptual model, defined by the author 'Aggregated Privateness Model', is now introduced.

### 2.1. The Aggregated Privateness Model

The Aggregated Privateness Model is represented by multiple clusters of private spheres, organized together to form complex structures, different among them, sometimes partially overlapping (see Figure 3).

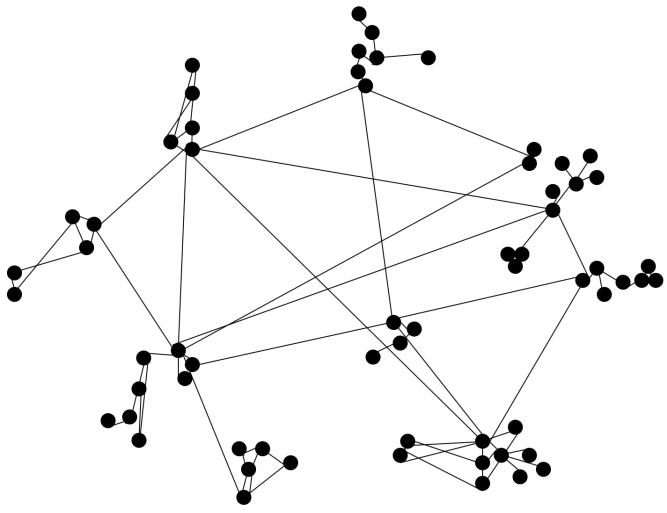

**Fig. 3.** A visual representation of the Aggregated Privateness Model.

The visual representation of the Aggregated Privateness Model has been inspired by the molecular composition of snowflakes. Each dot in the figure represents a private sphere. The different models and profiles in which the private sphere is intertwined are

represented by the clusters in the model (for example the musical preferences cluster of Figure 1 above), the 'edges' of a snowflake. They can be isolated, or connected to other clusters based on common features (in the example above, the model concerning musical preferences and the model concerning alcohol consumption preferences are connected). When the number of features shared by models increases, they are represented as partially overlapping, although still not completely identical due to the different purposes associated with each profile (for example marketing purposes versus healthcare ones). The connecting links among spheres and profiles represent the connecting features and elements shared within (and among) profiles. Their different length does not represent a property of the model, and is dictated only by reasons of composition. As explained above the Model is inspired by the molecular structure of snowflakes. It does, however, differ from it under certain perspectives. While a snowflake would present a symmetrical structure, the Model does not. This is because the informational structure and the clusters composing it do not originate all from a common element, but develop in a fashion that recalls that of distributed networks[12] with which, as will be explained below, it also shares certain dynamics. Just like the edges of a snowflake, individual private spheres are connected based on probabilistic predictions and models, and cooperate to create different forms and patterns. Such forms and patterns are influenced by how the molecules composing them combine, that is, by the information harvested in the private sphere and the way they are aggregated by machine learning, and by external factors, such as background knowledge or the crossing of data with other databases.

In addition to that, new models can build on previous models, just like snowflake and ice can keep growing. However, a snowflake leaves no trace once it melts. On the opposite, aggregated data structures are not so volatile, and their traces can last for long.

The uncertainty and flexibility also reflect on the informational structure. The snowflake Model, in fact, changes shapes constantly, and the patterns connecting its edges evolve. The models are expressly created to incorporate variables and weights, in order to be dynamic and respond to the new data collected within the house by the robots, or coming from other sources, such as the private spheres of other subjects. The reason for such dynamism is simple: a stiffening in the model would create unreliable profiles, not capable of reflecting the real preferences of the individuals, and therefore not useful or, worse, even prejudicial.

Furthermore, as briefly mentioned above, the Model has a structure similar to that of a distributed network. Similarly, within the Aggregated Privateness Model network mechanisms can occur. As highlighted by Actor Network Theory, within a network the communications among the nodes constituting it can affect the overall structure of the network itself, as well as the nodes and the connections between them[13]. The nodes of a network can, therefore, influence other nodes, the network (directly or indirectly) and the communication links among the nodes. These influences can be seen within the Aggregated Privateness Model as well, were the individuals, and their private spheres, can be influenced by the profiles they are associated with. In turns, however, individual preferences and behaviors can also modify the profiles and the models, which will, therefore, reflect differently on the other individuals also associated to the same profile. Such effect appears already at first, intuitive, sight and is also confirmed by the issues,

recently very popular among experts, concerning discrimination and bias in profiling[14]. In the case of the music preferences of individual A above, for instance, the songs listened to by A contribute to enrich the profile A belongs to, introducing different genres that are weighed by the mathematical rules used to create the model and used to adjust or change it. The changed model will be applied to other subjects, possibly new ones, that might in this way also be included in the structure, and so forth. However, these influences might also affect negatively the other subjects included in the profile, as will be better explained below.

Finally, just like ice, the Model can be at the same time opaque and transparent. The opacity is given not only by the presence of encryption and anonymization mechanisms before or after the processing that happens in the Cloud. It is also given by the fact that many profiles, being probabilistic, are non-distributive, and therefore might not disclose information concretely belonging to a subject. It implies that while certain characteristics of individuals are disclosed once the profile is associated with them, others might not be. In addition to that, each profile usually focuses on certain aspects, based on marketing interests, and do not necessarily represent, each, a complete picture of the individuals involved. This dichotomy between transparency, given by the many and detailed information available, and the opacity embedded in the probabilistic system tends, naturally, to dissolve. The more accurate the profiles are, the more distributive profiles are associated to individuals, and the more the individuals become identifiable through de-anonymization procedures.

Thanks to the Aggregated Privateness Model, and based on its three main features briefly explained above, two main consequences of the insertion of intelligent assistant robots within the house can be highlighted.

**De-contextualizing vs Re-contextualizing.** The first consequence concerns the positioning, at abstract level, of the house with regard to the private sphere of individuals. As seen in the previous paragraphs, historically the house was considered the physical *locus* of protection of the private sphere. After the insertion within the informational structure, the house becomes a node of the aggregation.

It is not the first time that the introduction of digital technologies is identified as causing a shift of the role and conceptualization of the house vis-á-vis the private sphere. Tracking and surveillance, in fact, have been deemed to cause a re-positioning of the house: decontextualized, it has become a point in the flow of movements which is the object of surveillance[15].

In parallel with the surveillance shift, the Aggregated Privateness Model shows how the house turns from the precinct of protection of private sphere to a node within a structure. According to the Aggregated Privateness Model, however, the presence of intelligent personal assistant robots, while potentially contributing to decontextualizing the house, also introduces a new context. Intelligent personal assistant robots, therefore, do not solely contribute to subtracting features from the house, as it occurs in the case of surveillance, but also add a new level, in which the value of the house intended as place of protection of the private sphere still plays a role. Following the path created by Prof. Nissenbaum's contextual privacy theory[16], the hive, the informational struc-

ture, becomes a context on its own[3]. Within the aggregated context, rules are represented by the algorithms creating the different models and aggregating the data that compose the structure. Unlike within the private or public spaces normativity is, therefore, retained by mathematical rules more than social or legal norms. The mathematical rules employed by the algorithms revolve around processing, that is aggregating data and identifying patterns. Origin of the raw data and the subsequent use of the aggregated data resulting from the processing are not, at the state of the art, contemplated by the rules existing within the Aggregated Privateness context.

At the same time, however, the information and data are still collected within the house, where individuals do have a certain expectation of protection offered by the location. In a subsequent moment, the additional information derived from those originally collected are deployed for multiple uses which the individuals are not aware of. There is, therefore, a dissonance between the expectations existing at the moment and place of collection (within the house) and the uses made of the information within and without the Aggregated dimension. Building upon Nissenbaum's theory, such dissonance creates an issue in terms of protection of the private sphere, a privacy issue.

Practical effects of this circumstance can be seen in the cases that more and more frequently find space in the discourse surrounding the use of profiling and automated decisions[17]. Nowadays many banks and financial institutions utilize software that analyze between six and eight thousand data points in order to grant or reject loan applications. Decisions can be influenced by, for example, purchase patterns, the time elapsed before accepting the terms and conditions of a website, musical preferences, alcohol consumption, healthcare data, and so on[18]. This circumstance shows how data collected within the context of the private sphere of the individual are used outside of the aggregated context, infringing the expectations of the subjects connected to the original collection. It is that infringement that creates, then, the ethical and moral disconcert surrounding such decisions. Another example can be found in the Alexa's stand in the murder trial, described above. In that case, in fact, the public prosecutor required the use of data collected within the house by the device. The collection of said data, however, is consented to by an individual based on the expectation that they would be necessary for Amazon's intelligent assistant robot to satisfy the user's requests. The

[3] The author acknowledges that several critiques have been moved to Prof. Nissenbaum's Contextual Integrity Theory. The theory has been often considered more focused on the common law system and therefore less relevant for the European context, especially with regard to data protection, or it has been seen as a complementary element of a bigger, general conceptualization of privacy and not a comprehensive, self-standing theory (see, among others, Michael Birnhack's review of Helen Nissenbaum's theory in Jurimetrics: Journal of Law, Science, & Technology, 52(4), 2011). While these limitations of the Contextual Integrity Theory are indeed valid, its relevance for this paper still stands. Since the paper presents an abstract conceptualization of the private sphere with regard to the use of intelligent robotics inside a certain context (the home), Contextual Integrity (whether alone or as part of a bigger theorization) provides a general framework of reference that highlights the connections among the private sphere, the physical and virtual environments with which it relates and, consequently, privacy and its protection.

use outside of said consent represents an infringement of the expectation, and creates a dissonance within the informational structure.

The practical consequences of the dissonance acquire importance once the Aggregated Privateness Model is used to test the solidity of the existing legislation concerning the protection of the private sphere, such as the European e-Privacy Directive[4][19] and the incoming General Data Protection Regulation[20]. Such test is, however, outside the scope of this paper, and should be the object of further research.

**A collective dimension of liability.** In addition to the issues connected to the contextualization of the aggregated dimension, the Model also provides conceptual clarity on a more collective dimension of the protection of the private sphere. Having acknowledged the abovementioned network mechanisms within the cluster, in fact, the Model helps shedding light on their consequences, the main one being that the behavior of the individuals composing the cluster affects this latter and the other 'nodes'. Readers consider this example: if the above mentioned individual A (with the relating musical preferences, age range, occupation, geographical location, etc.) asks for a loan and then fails to re-pay it, this might influence the entire profile A belongs to. As a consequence, individuals B and C, belonging to the same profile of A, might see their possibilities to obtain a loan decrease, or might face an increase in their interest rates.

The underlying idea is, indeed, not new. Since ancient times in small communities individual behaviors were deemed to influence the other members, as well as the 'good name' of the community itself. What is introduced by the Model is the application of an idea of indirect responsibility deriving from their behavior to individuals vis-à-vis other, unknown, individuals due to a connection based solely on the belonging to the same model or profile. Such responsibility, while it appears difficult to solve in terms of practical application, can be seen as a new form of Network Diffused Liability[21], a liability deriving from distortions cause not by a single dot in a network, but by the combination of the dots and their interactions with the environments they operate in; in other words, a liability of the network itself. It can serve as a basis to justify regulatory intervention to attempt redistributing such responsibility within the entire system, even if not pinning it to any individual in particular. In this way the Model, while acknowledging and conceptually framing a collective dimension of protection of the private sphere, a collective dimension of privacy[22], also acknowledges its practical limits. Such acknowledgement, however, does not lead to ignoring the issues deriving therefrom in day to day life, focusing on providing a comprehensive basis that can guarantee, in the practice, a uniform application of concepts that, otherwise, would make judges and authorities navigate at sight, grasping intuitive ideas to adjust the existing regulation.

In this regard, it is worth noticing that in the abovementioned Alexa case, the replies provided by the machine and for which the authorities sought mandate are not only

[4] Or the Regulation that will most likely take its place and whose text is currently being negotiated in the European Commission and with the member States, after being approved in the October 2017 by the Justice Committee of the European Parliament and the European Parliament itself.

tailored on the owner. Alexa's replies are also adjusted based on the profiles and models the owner is associated with, which means that the device's replies not only contain traits of the personality of the individual that Amazon's lawyers tried to protect invoking the First Amendment. They also contain influences from the other individuals included in the same profiles, whose data have also been used. This is where the positions of both the public prosecutor and Amazon, although both indeed solid, fall short of considering the implications of a more collective dimension of the private sphere, and its protection. Possible distortions, as highlighted by the examples before, can translate in severe consequences for individuals and their fundamental rights.

The Aggregated Privateness Model, although maintaining a conceptual and abstract dimension, can offer a uniform basis to limit possible distortions and damages to individuals in the subsequent practical application of provisions created to protect the very private spheres that compose the Model itself.

## 3. Conclusions

This paper introduced an abstract model to understand the concept and role of the private sphere, in relation to the introduction within the house of machine learning powered intelligent assistant robots. The model, called 'Aggregated Privateness', is elaborated with the purpose of offering a conceptualization that can serve as a basis for an analysis of the existing tools protecting the private sphere, Privacy and Data Protection in particular.

While the Model maintains its validity also in relation to different technologies, such as Ambient Intelligence and the Internet of Things in general, the starting point for its elaboration is the insertion inside the house of intelligent personal assistant robots. The presence of intelligent personal assistant robots in the house implies, in fact, the insertion of the robots inside the private sphere of the inhabitants. The Model shows how intelligent robots collecting data within the house insert the private sphere into an informational structure, at an abstract level.

A combination of multiple anonymous probabilistic profiles created with machine learning bundles on the individual additional layers of information. The aggregation of data for the creation of the different profiles corresponds to the aggregation of the private spheres of the individuals associated with the profiles.

As highlighted in the paper, the Aggregated Privateness Model sheds light on three main consequences of the interaction of the private sphere with intelligent robotics. The model explains how, within the cluster, the juxtaposition of distributive and non-distributive profiles creates a dichotomy between transparency (given by the information about individuals contained in the profiles), and opacity (due to the fact that not necessarily all that information concretely corresponds to individuals' preferences and behaviors). This seems to walk away from the general idea of the exposure of the life occurring inside the household environment. With regard to the collection of data for

commercial purposes, the walls of the house, while not necessarily made of glass, present a high level of permeability to the fluxes of information, and consequently to the statistical profiles built upon such information.

The model also helps explaining a flip in the role of the house. While this latter is decontextualized, the aggregation becomes a context by itself, with distinct rules. Due to the predominant role of machine learning, in the new context normativeness is given to the algorithm and its mathematical rules. Acknowledging the Aggregated Privateness as a context by itself can, therefore, help providing a conceptual basis for correcting some of the distortions such normativeness has created: discrimination and over/under inclusiveness. Once, in fact, the context is recognized, the deriving reasonable expectations of individuals can also be identified, offering support for the concrete application of provisions of law that still appear abstract, such as Article 22 of the GDPR on automated decisions. As explained by Nissenbaum's theory, the use of the information collected within a certain context outside of it breaches the rules and expectations connected to it. Similarly, the use of the information collected within the private sphere for a certain purpose and contained in the profiles for other circumstances, gives life to a mismatch between the expectations of the individuals providing the information and their effects.

Finally, the Aggregated Privateness Model helps grasping the weight and importance of the collective dimension of privacy and data protection. Once the individual is inserted in a cluster composed of anonymous profiles, the aggregation assumes a role in the protection of the private sphere of such individual.

Inside the cluster, each private sphere has the capability of influencing - and being influenced by - the other spheres, as well as the aggregation itself. The model highlights how, in turn, this translates into the circumstance that the behaviors of individuals inside their private spheres can affect other individuals, even without any relationships existing. This consequence of the use of probabilistic profiles which, as explained above, can also be interpreted in the light of ANT, opens the way to more collective dimensions of responsibility for the individuals inserted into a cluster. The paper has shown how the Aggregated Privateness Model works as a conceptual basis for the application of a form of Network Diffused Liability in the context of the protection of the personal sphere.

The combination of the dichotomy between opaqueness and transparency, the contextual use of the information contained in the aggregation, and the Network Diffused Liability within the clusters, can be used as conceptual bases to support the implementation of the existing legislation, such as the GDPR and the e-Privacy Directive in Europe, and avoid the distortions that have already been highlighted by experts and scholars. As shown by the Alexa role in the murder trial in the US, at stake are fundamental values and the protection of individuals, and while solutions can be developed in the span of a decade based on case law, the lack of a proper, uniform conceptual basis might amplify the discrepancies in the judicial and administrative decisions during such 'trial' period, penalizing and discriminating individuals. The Aggregated Privateness Model can provide such uniform basis with regard to the protection of the private sphere

in the age of intelligent robotics entering our houses, to help directing technological development on a desirable, responsible path.

## References


1. Amazon Echo Homepage, www.amazon.com/Amazon-Echo-Bluetooth-Speaker-with-WiFi-Alexa/dp/B00X4WHP5E, last accessed 2017/03/30.
2. Google Home Homepage, https://madeby.google.com/home/, last accessed 2017/03/30.
3. D6.2 Guidelines on Regulating Robotics, RoboLaw Project: Regulating Emerging Robotic Technologies in Europe: Robotics facing Law and Ethics, (2014).
4. Hansson, M. G.: The Private Sphere: An Emotional Territory and Its Agents. 1st edn. Springer, Dordrecht (2008).
5. Smith, R.E.: Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet. 1st edn. Sheridan, California (2000).
6. Shapiro, S.: Places and Spaces: The Historical Interaction of Technology, Home, and Privacy. The Information Society 14(4), 275-284, (1998).
7. Kumar, K.: Home: the promise and predicament of private life at the end of the twentieth century, in Public and Private in Thought and Practice, Weintraub, J. and Kumar, K. (eds.), 204-236, Chicago, (1997).
8. Case No. CR-2016-370-2, Circuit Court of Benton County, State of Arkansas (USA).
9. Vedder, A.: KDD: The Challenge to Individualism, in Ethics and Information Technology, 1: 275 (1999).
10. Hildebrandt, M.: Defining Profiling: A New Type of Knowledge?. 1st edn. Springer, Dordrecht (2008).
11. Costa, L.: Virtuality and Capabilities in a World of Ambient Intelligence: New Challenges to Privacy and Data Protection. 1st edn. Springer, Dordrecht (2016).
12. Sassen, S.: Digital Networks and the State: Some Governance Questions, in Theory, Culture & Society, 17(4), 19 - 33, (2000).
13. Latour, B.: On Actor Network Theory: a few clarifications plus more than a few complications. Soziale Welt, 47, 369-381, (1996).
14. Barocas, S., Selbst, A. D.: Big Data's Disparate Impact. California Law Review, 104, 671-732, (2016).
15. Bennett, C. J., Regan, P. M.: Editorial: Surveillance and Mobilities. Surveillance & Society, 1(4), 449-455, (2004).
16. Nissenbaum, H.: Privacy in Context: Technology, Policy, and the Integrity of Social Life. 1st edn. Stanford University Press, California, (2010).
17. Mendoza, I., Bygrave, L. A.: The Right Not to Be Subject to Automated Decisions Based on Profiling. Synodinou, T., Jougleux, P., Markou, C., Prastitou T., (eds.), EU Internet Law: Regulation and Enforcement. University of Oslo Faculty of Law Research Paper No. 2017-20. Springer, Dordrecht (2017, Forthcoming).
18. Goodman, B., Flaxman, S.: European Union regulations on algorithmic decision-making and a “right to explanation”. Presented at 2016 ICML Workshop on Human Interpretability in Machine Learning (WHI 2016), New York (2016).
19. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201 (2002).

20. Regulation (EU) 2016/679 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 (General Data Protection Regulation), OJ L119/1 (2016).
21. Teubner, G.: *Hybrid Laws: Constitutionalizing Private Governance Networks*. In Robert Kagan and Kenneth Winston (eds.), Legality and Community: on the Intellectual Legacy of Philip Selznick. Berkeley Public Policy Press, Berkeley (2002).
22. Taylor, L., Floridi, L., van der Sloot, B. (Eds.): Group Privacy: New Challenges of Data Technologies. 1st edn. Springer, Dordrecht (2017).