Prescient (Berlin, Nov. 2012)

Robots in the Sky with Privacy: A New Threat to Data Protection?

Ugo Pagallo (Law School, Torino)
Outline

1. Introduction: The Complexity of Robotics
2. Network-Centric Applications
3. Personal & Domestic Robots
4. The Transparency of Data Processing
5. The Opaqueness of Privacy
6. Levels of Access and Control over Info
7. The Troubles with Consent
8. Conclusions
1. Introduction

In order to grasp how robotics may affect privacy and data protection, let’s start with the complexity of this field...
Think about...

**Drones**

**Driverless Cars**
Think about...

Unmanned Underwater Vehicles

Industrial Robots
Think about...

Adam the Scientist

HRP-4C
1. Introduction

Here, focus is on the class of robots that are connected to a networked repository on the internet that allows such machines to share the information required for object recognition, navigation and task completion in the real world.
2. Network-centric Apps

Think of a network and database repository where machines can share information and learn from each other about their behaviour and their environment. Avoiding shortcomings of traditional approaches, such as on-board computers for robots, the goal is to complete a sort of cloud robotics infrastructure with all that is needed to close the loop between robots, RoboEarth, and robots.
2. Network-centric Apps

[Diagram showing the flow of data and processes involving object scanning and detection.]
2. Network-centric Apps

Within the class of network-centric apps, let me restrict the focus of the analysis, so as to dwell on the sub-class of network-centric robots for personal and domestic use...
3. Personal & Domestic Robots

We already have, after all, a number of robot toys and robot nannies that are programmed to provide love and take care of children and the elderly.
Moreover, think of new types of artificial assistants for university teachers, that could help us schedule a set of conferences, lectures and meetings: i-Jeeves could directly accept invitations, book hotel rooms, flights and so forth...
3. Personal & Domestic Robots

In light of such network-centric robot apps for personal and domestic use, we have to tackle a twofold problem...

Although connected, issues of data protection and privacy should be examined separately. Let’s start with the “transparency” of data processing as opposed to the “opaqueness” of the individuals (Arendt 1958)
3. Personal & Domestic Robots

In light of such network-centric robot apps for personal and domestic use, we have to tackle a twofold problem...

Although connected, issues of data protection and privacy should be examined separately.

Let’s start with the “transparency” of data processing as opposed to the “opaqueness” of the individuals (Arendt 1958)
3. Personal & Domestic Robots

In light of such network-centric robot apps for personal and domestic use, we have to tackle a twofold problem...

Although connected, issues of data protection and privacy should be examined separately.

Let’s start with the “transparency” of data processing as opposed to the “opaqueness” of the individuals (Arendt 1958)
4. Transparency

As to current rules of data protection, a new generation of network-centric applications could collect data incessantly and in ways that are “out of control,” because such machines are increasingly “autonomous.”
4. Transparency

More precisely, some types of robots are:

• **Interactive**, as they do perceive their environment and respond to stimuli by changing the values of their own properties or inner states

• **Autonomous**, because they modify their inner states or properties without external stimuli, thereby exerting control over their actions without any direct intervention of humans; and

• **Adaptable**, for they can improve the rules through which their own properties or inner states change
4. Transparency

More precisely, some types of robots are:

• Interactive, as they do perceive their environment and respond to stimuli by changing the values of their own properties or inner states

• Autonomous, because they modify their inner states or properties without external stimuli, thereby exerting control over their actions without any direct intervention of humans; and

• Adaptable, for they can improve the rules through which their own properties or inner states change
More precisely, some types of robots are:

- **Interactive**, as they do perceive their environment and respond to stimuli by changing the values of their own properties or inner states.

- **Autonomous**, because they modify their inner states or properties without external stimuli, thereby exerting control over their actions without any direct intervention of humans; and

- **Adaptable**, for they can improve the rules through which their own properties or inner states change.
4. Transparency

By collecting information in open or public environments and, moreover, bringing such environmental information to cloud servers, robots can severely impinge on current data protection, since these machines may replicate and spread all the data they collect beyond human control...
Curtis Karnow proposed this latter scenario in his seminal 1996 paper where he considers an “intelligent programming environment which handles air traffic control” such as “Alef.” Rapid advancement of robotics makes this scenario more than realistic...
4. Transparency

No judge can isolate the ‘legal’ causes of injury from the pervasive electronic hum in which they [robots] operate, nor separate causes from the digital universe which gives them their mutable shape and shifting sense. The result is a snarled tangle of cause and effect as impossible to sequester as the winds of the air, or the currents of the ocean (Karnow 1996)
4. Transparency

To be sure, several of such data protection issues do not only belong to robotics network-centric applications, since they rise in other fields such as ambient intelligence or ubiquitous computing.
4. Transparency

However, in addition to problems of data protection induced by "autonomous machines," personal and/or domestic robots will raise a number of psychological issues concerning feelings of subordination, attachment, trustworthiness, etc.
4. Transparency

Moreover, a new generation of robot nurses, robot nannies, smart robot toys, or i-Jeeves 2.0 will do know a lot of things about our private life... What’s at stake here mainly concerns people’s “opaqueness”
5. Opaqueness

Indeed, people’s privacy has often to do with the idea of opacity (Arendt 1958), *i.e.*, privacy conceived of as a condition of “solitude,” “exclusion,” “secrecy,” etc. (Westin 1967; Gavison 1980; Allen 1988; and so forth)
5. Opaqueness

All in all, it is likely that individual interaction with personal machines, domestic robots, and so forth, will affect what U.S. common lawyers call a reasonable “expectation of privacy” (Katz v. United States, 389 U.S. 347 (1967))
5. Opaqueness

We can update the US SC’s ruling, stressing that “the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. . . . But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.”
6. Levels of Access and Control

Although they should be differentiated, *e.g.*, Articles 7 and 8 of the EU Charter of Fundamental Rights, matters of data protection and privacy at times overlap, as it occurs with people unintentionally using network-centric machines that infringe data protection laws, *i.e.*, regardless of human wrongdoing or mere negligence.
6. Levels of Access and Control

In addition, think of people spying on other individuals through domestic robots, and even kidnapping such robots so as to get personal data.
6. Levels of Access and Control

In most of the cases, some approaches to data protection, such as “privacy by design,” appear particularly fruitful to protect people’s “opaqueness”
6. Levels of Access and Control

According to PbD approaches, in fact:

- Personal data should be automatically protected in every IT system as its default position.
- Data protection should accordingly be embedded into design.
- A cradle-to-grave, start-to-finish, or end-to-end lifecycle protection ensures that privacy safeguards are at work even before a single bit of information has been collected.
- (...)
6. Levels of Access and Control

According to PbD approaches, in fact:

• Personal data should be automatically protected in every IT system as its default position

• Data protection should accordingly be embedded into design

• A cradle-to-grave, start-to-finish, or end-to-end lifecycle protection ensures that privacy safeguards are at work even before a single bit of information has been collected

• (...)


6. Levels of Access and Control

According to PbD approaches, in fact:

- Personal data should be automatically protected in every IT system as its default position.
- Data protection should accordingly be embedded into design.
- A cradle-to-grave, start-to-finish, or end-to-end lifecycle protection ensures that privacy safeguards are at work even before a single bit of information has been collected.
- (…)

(...)
According to PbD approaches, in fact:

- Personal data should be automatically protected in every IT system as its default position
- Data protection should accordingly be embedded into design
- A cradle-to-grave, start-to-finish, or end-to-end lifecycle protection ensures that privacy safeguards are at work even before a single bit of information has been collected
- (...)
6. Levels of Access and Control

Back to the example of people kidnapping domestic robots so as to get personal data, we can accordingly program such machines with a remote control switch-off device...
6. Levels of Access and Control

However, such automatic approaches to the principle of privacy by design fall short in coping with a number of further critical cases...
7. The Troubles with Consent

Informational privacy and the traditional “right to be let alone” (Warren and Brandeis 1890) do not represent any automatic zero-sum game, because personal choices play a crucial role when individuals modulate different levels of access and control over information, depending on the context and its circumstances (Nissenbaum 2004).
7. The Troubles with Consent

Accordingly, some approaches of the aforementioned principle of privacy by design may fall short in coping with issues that depend on the cultural context and the type of application with which we are dealing: robots as “lovers” (Levy 2007), as “human cubs” (Dautenhahn 2007), as “pets” (McFarland 2008), and so forth...
Think of the robot-centred HRI approaches, where the emphasis is on the “robot as a creature, i.e., an autonomous entity that is pursuing its own goals based on its motivations, drives and emotions” (Dautenhahn 2007: 683)
7. The Troubles with Consent

Although the “social needs” of the robot are defined by the designer and modelled by the internal control architecture of the machine, it is the user that enables the robot to “survive in the environment” by fulfilling its needs.
7. The Troubles with Consent

By treating the machine as an autonomous entity pursuing its own goals based on its motivations, humans indeed have to satisfy its social drives by singling out and responding to the robot’s internal needs.
7. The Troubles with Consent

Summing up:

• The main legal issue will often revolve around how humans educate, treat, or manage their personal or domestic robots, rather than around who owns, builds or sells them.

• Moreover, we should distinguish between robots as pets, assistants, AI kids, lovers, etc., since humans will modulate different levels of access and control over information, according to the different type of personal or domestic robot.
7. The Troubles with Consent

Summing up:

• The main legal issue will often revolve around how humans educate, treat, or manage their personal or domestic robots, rather than around who owns, builds or sells them.

• Moreover, we should distinguish between robots as pets, assistants, AI kids, lovers, etc., since humans will modulate different levels of access and control over information, according to the different type of personal or domestic robot.
8. Conclusions

The challenges of robotics technology and, more particularly, the class of network-centric apps for personal and domestic use, suggest a final convergence between privacy and data protection...
8. Conclusions

What “robots in the cloud” will ultimately affect concerns the “ontological friction” in the informational sphere, namely the forces that oppose the flow of personal information, as “the amount of work and efforts required for a certain kind of agent to obtain, filter and/or block information (also, but not only) about other agents in a given environment” (Floridi 2006)
8. Conclusions

Whilst some “degrees of friction” are required to keep firm distinctions between agents and system, individuals and society, robots will affect such degrees in a twofold way, that is, via new expectations of privacy in the personal or domestic human-robot interaction that reverberate on the ways in which personal data ought to be processed through different types of network-centric applications.
8. Conclusions

Whilst some “degrees of friction” are required to keep firm distinctions between agents and system, individuals and society, robots will affect such degrees in a twofold way, that is, via new expectations of privacy in the personal or domestic human-robot interaction that reverberate on the ways in which personal data ought to be processed through different types of network-centric applications.
8. Conclusions

Whilst some “degrees of friction” are required to keep firm distinctions between agents and system, individuals and society, robots will affect such degrees in a twofold way, that is, via new expectations of privacy in the personal or domestic human-robot interaction that reverberate on the ways in which personal data ought to be processed through different types of network-centric applications.
A new category of artificial behaviour, neither simply mechanical nor reducible to human beings as the source of their action, will produce multiple relevant effects in the fields of privacy and data protection...
8. Conclusions

Since robots are here to stay, the aim of the law should be to wisely discipline our mutual relationships.
THANK YOU VERY MUCH!

ugo.pagallo@unito.it

(University of Torino, Italy)
References