Cloud services for robotic nurses? Assessing legal and ethical issues in the use of cloud services for healthcare robots *

E. Fosch-Villaronga, H. Felzmann, M. Ramos-Montero and T. Mahler

Abstract— This paper explores ethical and legal implications arising from the intertwinemment of cloud services, healthcare and robotics in recent developments towards increasing reliance on cloud-based services for healthcare robots. It closes an existing gap in the literature by highlighting the distinctive ethical and legal concerns associated with the inter-dependence of the cyber- and the physical aspects of healthcare cloud robotics. The identified core concerns include uncertainties with regard to data protection requirements; distributed responsibilities for robot behavior; the achievement of transparency and meaningful consent for cloud robot services especially for vulnerable robot users; secondary uses of cloud data derived from robot activities; data security; and wider social issues such as the digital divide and the assignment of responsibilities for social consequences to robot designers. The paper aims to raise awareness and stimulate reflection with regard to the legal and ethical impacts on different stakeholders arising from the use of cloud services in healthcare robotics. It shows that due to the complexity of these concerns the design and implementation of such robots in healthcare requires an interdisciplinary development and impact assessment process. In light of legal requirements and ethical responsibilities towards end-users and other stakeholders, we draw special attention to practical considerations that engineers should be cognizant of when developing cloud services for robots in the healthcare field.

I. INTRODUCTION

Increasingly, robots have transformed from tools designed for highly specific tasks to multipurpose information hubs that are highly connected with their environment and are characterized by complex distributed information flows [1]. In the area of health robotics, there is a movement towards increasing integration of robot functionalities with electronic health records (EHR), the Internet of Things (IoT) and wider Ambient Assisted Living (AAL) systems. The development of cloud robotics adds complexity with regard to further complications of resulting information flows. The combination of complex connected information flows in the background and the physical presence of robots vis-à-vis human users in the foreground is transforming the ethical challenges that the emerging field of healthcare robotics is likely to encounter in the future; however this type of concern has yet to be reflected in the robot ethics literature. Similarly, the duality of a visible physical presence and the less-visible processing of personal data represents a challenge for acquiring consent and, more generally, complying with data privacy laws.

The concept of cloud robotics is said to have been introduced in 2010, when Kuffner outlined the potential of robots to rely on data or code from a network to support their operations, rather than having all sensing, computation and memory integrated into a single standalone system [2]. The reliance on the cloud has the potential to offload heavy computing tasks and to allow robots to draw on shared knowledge databases [3–4], including reusable libraries of robot knowledge [5–7], skills or behaviors that would allow them to manage complex situations without having been explicitly programmed to do so [8]. This lightens the weight of the robot, allows better robot performance, and thereby allows cheaper physical embodiment, which is advantageous for engineering as well as market purposes.

Notwithstanding these and other benefits, the use of cloud services in robotics does not come without drawbacks. Cloud computing encompasses various deployment models and may involve multiple service layers and service providers, with supply chains that are often opaque [9]. Such complexity can give rise to significant challenges in relation to control, security, and risk management [10]. The migration to the cloud also requires addressing a range of classical and new data protection issues including data safety, divergent cross-national data security requirements, and complexities of achieving user transparency and consent, data portability, right to be forgotten or the privacy-by-design and by-default enshrined in the General Data Protection Regulation (GDPR). Moreover, distributed responsibilities for robot functioning and robot safety, and social implications with regard to the availability and use of cloud services in different sections of society require attention.

Given the comparatively recent development of cloud robotics, however, the literature is still short on studies addressing the intertwinemment between cloud, robots and healthcare. The aim of this paper thus is to explore the ethical and legal implications of the use of cloud services for healthcare robots. We argue that the insertion of a robot in healthcare institution is not straightforward and that an impact assessment should be carried out. In this respect, we
identify a number of concerns that may have to be thought through before the effective implementation of the robot, in particular consent and distribution of responsibility. We also address issues likely to require attention in the future: the increasing dependence of cloud services for robot technology or the increasing digital divide. We draw special attention on practical considerations that engineers should be cognizant of in developing cloud services for robots in the healthcare field, in light of legal requirements and ethical responsibilities towards end-users and other stakeholders. The paper aims to raise awareness and stimulate reflection with regard to the legal and ethical impacts the use of cloud services for robotics in healthcare pose to different actors.

II. CLOUD ROBOTICS IN HEALTHCARE

Ibana was probably the first to anticipate cloud robotics when he wrote in 1997: “a remote-brained robot does not bring its own brain with the body. It leaves the brain in the mother environment, by which we mean the environment in which the brain’s software is developed, and talks with it by wireless links [11].”

Cloud computing has now become mainstream and the boundaries between cyber and physical are becoming increasingly blurred. Cloud computing essentially involves the use of computing resources over a network, typically the Internet, scalable according to demand. The National Institute of Standards and Technology has defined cloud computing as a “model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources [...] that can be rapidly provisioned and released with minimal management effort or service provider interaction [12].”

Connecting the robot to the cloud has certain advantages: it provides a shared knowledge database, heavy computing tasks can be offloaded, and a reusable library of skills or behaviours to map perceived complex situations can be created [2, 13]. The concept of cloud robotics has since been extended to cover “any robot or automation system that relies on data or code from a network to support its operation, i.e. where not all sensing, computation and memory is integrated into a single standalone system [14].”

Roboticians with requirements to process large quantities of data now have ready access to cloud robotic platforms which can greatly facilitate access to relevant resources, information and communications [15]. The RoboEarth project (2010-2014) developed a “Cloud Robotics infrastructure, which includes everything needed to close the loop from robot to the cloud and back to the robot.” The catalyst for the project was the assumption that at that time near future robots would need to “reliably perform tasks beyond their explicitly pre-programmed behaviours and quickly adapt to the unstructured and variable nature of tasks [5];” something unlikely without a cloud platform.

RoboEarth demonstrated that the use of a cloud system could create an environment where robotics knowledge and information can be shared to enhance robot performance and to enable knowledge sharing independently of robotics architecture. In addition, Waibel et al. argued that cloud may also facilitate component reuse across different systems and developers, and the leveraging of expertise about the usage, robustness, and efficiency of components [16]. This approach has since been used to make standalone robots outperform their previous capabilities, for example by engaging better with children, or assisting the elderly in a much more natural way [17-19].

Another example of cloud platforms for Robotics is RAPP (Robotic Applications for Delivering Smart User Empowering Applications). It is a European research project (2013-2016) which has developed an open source software platform focused in people at risk of exclusion, e.g. elderly [3]. One of the ways to help this sector of the population is using assistive robots. With these bases, they designed a framework with a cloud-based approach, integrating robotic devices and their applications [4]. This allows to support a wide range of robots and make them more useful with less hardware requirements. Besides, they have shared a wide variety of tools to develop your own applications, independently of the operative system, store them and share them, confirming the idea RoboEarth started.

One application domain where it is likely that this technology will be increasingly adopted is the healthcare domain where the use of robots is on the increase. The European Commission’s Robotics for Healthcare Roadmap defines healthcare robotics as “the domain of systems able to perform coordinated mechatronic actions (force or movement exertions) on the basis of processing of information acquired through sensor technology, with the aim to support the functioning of impaired individuals, medical interventions, care and rehabilitation of patients and also to support individuals in prevention programs”. A particularly prominent area of development are healthcare robots that interact cognitively and socially with humans in healthcare environments, including, for example, projects that aim to foster child well-being in medical facilities through engagement with pet robots [20], provide robots for assistance or companionship in elderly care [19] or employ robots for educational purposes [21].

For example, MARIO (Managing Active and healthy aging with use of caRIng servIce rObots) is a European project which has developed a multifunctional care robot to assist people with early to moderate dementia in maintaining their independence and social connectedness at home, hospitals or nursing homes. Many of the functionalities (navigation, speech to text, text to speech, games, etc.) run locally (on the robot), however, for several functionalities MARIO requires internet connection. While traditionally in hospitals, patient data is stored locally in internal networks, in health robotics functionalities frequently rely on internet connectivity and increasingly on cloud connectivity. This constitutes a substantial change in the nature of data flows, raising specific privacy and security concerns [1].

Healthcare is not limited to hospitals and care homes, but also domestic care. The number of domestic robots that we can find in the market with healthcare applications is very varied. Each one offers different features, however, what they have most in common is their ability to connect to the cloud. Zenbo can react in emergency cases – when the owner falls
down and calls the relatives. Unibo from Unirobot Corporation in collaboration with Fujitsu uses the cloud to talk and interact in a more natural way with people. Unibo also uses facial recognition, emotions or even voice-emotion to know how your state is.

![Figure 1 On the left, Zenbo robot from Asus. In the middle, NAO, a robot used to test the RAPP project. On the right side, Unibo from Unirobot Corporation](image)

**III. LEGAL AND ETHICAL CONSIDERATIONS**

The literature on legal and ethical issues in healthcare robotics has an overly strong focus on the robot itself and largely ignores background information processing; the literature covering cloud computing lacks attention to human-machine interactions, which are associated with distinctive ethical and legal concerns in the field of cloud computing and robotics.

Weng and Zhao were among the first to draw attention to this particular problem. They investigated legal and regulatory issues of networked robotics in 2011 and argued that cloud-enabled networked robots could transfer risks bidirectionally between the physical and digital worlds, and that this would present greater challenges to regulatory frameworks than was hitherto the case with standalone robots [22]. The authors explained that the dual nature of cyber-physical systems might hinder the identification of the origin of a problem, the calculation of its consequences, and its subsequent future impacts. How do these concerns manifest themselves in the healthcare domain?

Cloud robotics raises particular challenges with regard to the implications of human-robot interactions, as they combine physical embodied robotic systems that interact with the user with complex (and invisible) distributed data flows in the background. Users are known to generally relate easily to the physical robot with which they interact. However, in cloud robotics it is not transparent to the user that the physical robot itself is not the only relevant unit in the interaction, but that significant aspects of its functioning are based elsewhere. This distributed cyber-physical setup brings multidisciplinary challenges and emerging concerns that will be addressed in the following sections.

A. Without further guidance, the General Data Protection Regulation might be difficult to be applied to cloud healthcare robotics

The upcoming General Data Protection Regulation (GDPR) will provide challenges to healthcare robotics in many ways [23]. Some of the rights addressed by the GDPR include privacy-by-design (Art. 25 GDPR), which will oblige the data controller, at the time of the determination of the means for processing and at the time of the processing itself, to implement appropriate measures for ensuring that all the requirements of the GDPR are met. However, the regulation remains silent on what exact measures should be implemented, e.g. a programming language that embeds privacy policies in the code [24]. Relevant literature on privacy by design argues that to meet these requirements measures taken need to be pro-active, as a default setting, embedded into the design, with full functionality, offering a full lifecycle protection, and being open and user-centric [25]. The complexity of the cloud robotic system makes it challenging to comply with this principle in practice.

Other rights that will pose challenges are the right to erasure (alias right to be forgotten, Art. 17 GDPR), especially in machine learning environments [26]; the right to data portability (Art. 20 GDPR), because using data in a “commonly used and machine-readable format” may increase security issues; and the right to object and automated individual decision-making (section IV, including Art. 21 and Art. 22), especially because not only may robots be deciding autonomously continuously, but also because under some circumstances interrupting the robot’s decision-making to ensure compliance with this requirement may imply a greater risk than just continuing with its usual functioning. This may be aggravated in the case of healthcare robots, which due to their specific purpose and user groups may have to consider trade-offs between compelling interests such as privacy vs. surveillance, safety vs. free will. In particular, this challenges the classic requirement of informed consent: first, because the robot might have to ask for consent very frequently to meet requirements, which would be unduly burdensome and disruptive; and second, because for some user groups, such as older persons or persons with dementia, the mental condition of the user may deteriorate over time, which may require rethinking how consent is obtained from the user and how evolving user preferences can be captured.

The complex interplay between legal compliance and legal enforcement also comes to the fore in cloud robotics, due to peculiarities of the configuration of the GDPR, with regard to how strict the consequences for violation are - criminal charges and up to 4% of the total revenue of the company - and how vague the requirements for both compliance and enforcement are. As outlined above, there are significant complexities and uncertainties regarding how compliance with GDPR requirements can be ascertained and when penalties will be applied. Standard initiatives as the recent ISO/IEC 19134:2017 on Guidelines for privacy impact assessment could help understand more concretely how the data controller or processor could comply with the data protection regulation, potentially also easing the law enforcement process. Even recent accountability tools - like the one released by CNIL - could shed light on this problem and speed up the accountability and enforcement process. In practice, the regulator currently struggles to translate the abstract idea of privacy into concrete techno-rules [27].

Additional clarity on the requirements is required, for instance with regard to (i) complex ecosystems - cloud, or even cloud of clouds -, (ii) specific types of users – while the GDPR mentions children as worthy of particular protections
due to vulnerability, it does not explicitly identify other relevant groups in healthcare settings as vulnerable such as elderly or infirm people, and (iii) types of data—specific raw and metadata requirements need to be explicitly identified to facilitate a better response to the complexities of their interplay.

One further challenge with regard to meeting data protection requirements is due to the distributed nature of cloud robotics. While the physical robot might be located in one jurisdiction, the cloud providers may be located in different jurisdictions with potentially diverging data protection requirements. With physical robots seemingly located in a clear location, it may become obscured to users as well as regulators that data processing might take place somewhere else in the world, and, depending on the particular setup, potentially in multiple locations.

After the Safe Harbor Decision was declared invalid in the Maximilian Schrems v Data Protection Commissioner Case C-362/14, there has been a lot of concern on what is the territorial scope of the new Data Protection Regulation and how third countries can show an adequate level of protection to the processing of personal data. The GDPR is clear on its territorial scope: ‘this Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not’ (Art. 3.1 GDPR). The Art. 3.2 GDPR adds that activities offering goods and services - including the use of offering cloud services and monitoring behavior that happens in the Union – will also be part of the protected scope of the regulation. Concerning the U.S., there is a new framework called Privacy Shield, which establishes the requirements to follow for these two countries.

**B. Identifying the data controller and data processor roles and their responsibilities might be difficult in cloud robot ecosystems**

As there are multiple players in such ecosystems including robot users, software developers, cloud service providers, and hardware manufacturers, chains of responsibility may be extensive and complex. At first sight, availing of cloud-based Platform as a Service (PaaS) appears fairly straightforward from a legal and regulatory point of view, in that most well established cloud-service providers (IBM, Google, Amazon) target mobile phones and web-applications which are generally considered well-regulated [29]. However, a robot is a very different entity from a smartphone; a robot has audio-visual sensors (cameras and microphones) which could potentially function *all the time* with or without the user's consent, and they perform a multitude of operations, ranging from face recognition, face detection, human detection to object detection, scene understanding or environment mapping. Therefore, a robot operating in an environment must perceive all the sensory data that its sensors allow it continuously. It also translates these into self-initiated action, including motion or interaction with end users. The processing of such information, when using cloud robotics, is not done on-board the robot, but often on a third-party cloud service provider.

In this set-up there is a need to define clearly the roles and entities involved in such an ecosystem:

- The PaaS cloud provider
- The physical robot
- The owner of the robot, which may be different from the user, including the hospital or the care facility
- The person, organisation or legal entity which has built the software and/or maintains it with access to PaaS
- The end user of the robot
- The various parts that configure the robotic system, such as wearables or ambient intelligent technologies.

![Figure 2. Entities and roles in healthcare robot using cloud services](image)

According to the Art. 4.7 GDPR the *controller* is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. In the case of cloud robotics, there are various candidates for this role: the controller could be the developer of the software that controls the robot, and/or the person responsible for operating the robot, starting the software and maintaining it, as well as the end user. The role of the *processor* may also be difficult to identify definitively, especially in Robot-as-a-Service environments [30]. The Art. 4.8 GDPR defines the controller as the natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. In the case of cloud robotics, that entity is normally the PaaS provider, but this may largely depend on how the robot is configured, e.g. whether the robot includes applications from other providers or whether it has access to other technologies processing data, too.

In order to address the challenges arising from the complexity of players and components, it will be essential to identify the precise interactions and communications between the different players, such as for instance robot2robot, wearable2robot, robot2cloud, person2robot, sensors2cloud, sensors2robot. This mapping may be relevant for understanding robot learning processes – regarding source of information, trust and security – but also for a clear division of responsibilities, which should be carefully modelled and detailed in a contract between the different providers and

---

**References**

[29] IBM, Google, Amazon

[30] Robot-as-a-Service
needs to take account of the complexity of the relationship between the players.

**C. Realizing transparency and achieving meaningful user consent is particularly challenging for cloud robotics in healthcare**

Users of information technologies should receive sufficient information on the implications of using the technology, especially in light of the non-explicit-but-highly-debated right to explanation enshrined in the recital 71 of the GDPR [31]. This right refers to facilitating understanding of the autonomous decision-making of the machine - healthcare robots in our case - and obliges the controller to give an explanation of the decision arising from autonomous assessments by the robot and to allow users challenges to such decisions. Achieving such meaningful understanding is challenging with regard to any information technology, given that the use of data enabling practical functionalities (or additional data uses for further purposes) remains hidden behind the user surface. For robots, it is particularly challenging as they are intuitively perceived by users as physical entities with a clear location, rather than as systems with potentially highly distributed information flow, i.e. using cloud services from various providers.

Providing transparency of data uses to end users is a necessary precondition for achieving informed consent. However, achieving meaningful consent is demanding. Consent requires meeting these criteria [32]: (i) user capacity to understand information and make decisions, (ii) voluntariness of the user's consent, who needs to have a choice and not be coerced in their decision-making process, (iii) adequate provision of information relevant to decision-making, including risks, benefits and costs, (iv) achievement of understanding of the information, (v) decision and (vi) authorization.

With regard to cloud robotics for the healthcare context, the achievement of transparency and consent encounters a number of challenges with regard to these criteria. Many of the care robots currently under development are developed specifically for vulnerable populations with less capacity than average adults, such as persons with dementia or children with autism. It is also likely that the encounter of users with those robots takes place in residential or care settings where potentially coercive power dynamics might be at play, affecting both care recipients and their decision-making representatives who may feel they have no choice but agree to the use of robots in their care. These challenges to meeting preconditions of consent impact how effectively information can be communicated and put to use in users' decision-making. With regard to cloud robotics, what is particularly challenging is providing accurate but accessible information about the nature of the robot's information processing. The representation of complexities of data processing in such ecosystems is compounded by the potential lack of transparency even to those responsible for communicating with end users, for instance with regard to the exact implementation of service provision or potentially varying conditions for subcontracted elements, resulting in uncertainties regarding who provides which aspect of services, where those services are located and what potential risks are associated with them.

More clarity is needed regarding transparency requirements for data flows and data use by service providers, whether towards end-users or providers who are availing of subcontracted services. Only once such information is made easily available will it be possible to develop standards of good practice for informing end users of the implications of availing of cloud robotics services.

**D. Robot metadata as a cost-effective solution that may challenge transparency and user rights**

Another area of concern that has been previously underexplored with regard to the area of cloud robotics is the potential retail of anonymized and aggregated meta-data, a common practice and business model in many online services (including major players such as Facebook). Following this model would mean that the PaaS provider might retail metadata acquired from robots to third party customers (such as advertising companies). Due to the high cost of operating a PaaS cloud service (on average $0.90 an hour when using high performance cloud instances such as Amazon AWS), PaaS providers have to either charge for the service, or offer it for free, and rely on earnings from the data-mined metadata acquired from robots.

While a multitude of online services work with this business model, it has been extensively criticized, not least with regard to frequent lack of transparency to users as to how their data is being used. The use of this business model in the context of healthcare robots is particularly problematic, given the sensitivity of health related data coupled with the scope and extent of data collection (including data from the intimate sphere of users, as collected especially by domestic care robots), and the resulting potential complexity and reach of information that could be derived from such data. What is particularly problematic in this context is the potential vulnerability of users which may raise additional concerns with regard to the utilization of data derived from such robots. It would need to be clarified whether transparency and opt-out requirements in this context would potentially exceed transparency requirements in other commercial contexts, due to the particularly sensitive nature of the data used.

**E. Cloud robotics raises increased data security challenges**

Data security is a particularly significant concern for cloud robotics. With the move to the cloud, additional information transfers between different entities are taking place, with a correspondingly higher risk of data breaches. It is paramount that clear responsibilities for data security are assigned and that appropriate processes are in place to identify and communicate any emerging risks or breaches. Technological solutions to data security also need to be data protection compliant, i.e. they should ensure an adequate level of protection of personal data, including all the requirements of Art. 32 GDPR: pseudonymization and encryption of personal data; ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, which may be particularly significant in light of the vulnerability of many
users of healthcare robots; but also ensuring a way to regularly test, assess and evaluate the effectiveness of technical and organizational measures for ensuring the security of the processing.

Current industry security standards use the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) [33-34]. Both are protocols for data encryption and authentication, creating a secure connection in an unsecured network, use a handshake procedure, and encrypt the data between endpoints (in this scenario, the robot and the cloud). However, those protocols have been known to have weaknesses in the past such as the POODLE attack [35], and although most weaknesses are rectified and the security protocols withstand various public attacks, highly sensitive data (e.g., private medical information) transmitted could potentially be intercepted. Due to the scheme of PaaS (client-server paradigm) even though the PaaS provider has to support high encryption and security protocols and standards, ultimately it remains with the data-processor (software or robot owner, developers and manufacturers) to ensure that the highest possible security standards are being used correctly.

The exchange of data from the device (robot) to the PaaS endpoint (cloud) must also be secured and this will most often be the responsibility of the data-controller (developer or owner) as the process flow is always initiated from the device to the cloud.

In healthcare clouds, extra security and privacy requirements are needed. Zhang [36] provided and analyzed security requirements for generic healthcare clouds, while Deng et al. performed a similar analysis for the specified case of home healthcare applications in the cloud [37]. Both mentioned the necessity of physical and network security, as outlined previously. Concerning the security of the patient’s data, the following points should be considered:

- Patient-centric transparency. Patients should know their privacy rights and be able to specify and delegate the access control policy of their data.
- Data-centric protection. It is unknown who is going to require the information (family, doctor, emergency services, hospital, etc.), therefore the data distribution and usage has to be controlled.
- Emergency access and availability. For emergency cases, medical data should be temporarily available for any person who is helping the patient.
- Data confidentiality. Access control needs to be secure and efficient and “potential side channel leakage of medical data should be prevented” [37].

F. Cloud robotics creates additional areas of responsibility for robot safety and security

A closely related, but distinct point is the issue of robot safety which could be compromised if data security is not ensured, but which could also be affected by other factors relevant in cloud robotics. This is particularly important because of the shift from a mere data storage cloud to an active cloud where all the decision-making processes for robot behaviour happens [5]. This is going to be crucial for robot learning, and raises questions such as who is responsible for ensuring that the robot’s learned behaviour is appropriate for safety reasons. It is also significant for the management of distributed and shared responsibilities, especially if a responsibility of the provider of new information and skills in the cloud is considered [38].

Because distributed processing in cloud environment implies the involvement of different parties and thus having different responsibilities for the functioning of the robot, it will have to be clear what level of accountability each robot engineer has and how it is going to be determined who is responsible for ensuring the robot’s safety. This is particularly significant given the intended uses of healthcare robots developed for vulnerable populations.

G. Wider societal issues

In addition, some wider social implication need to be considered with regard to cloud robotics. According to the European Parliament, robotics engineers should remain accountable for the social, environmental and human health impacts that their creations may pose to present and future generations [38]. While this resolution shows awareness of the need to address the significant social impacts arising from technology development, the technological professions are currently ill prepared to manage such requirements. In light of such developments, increased attention will also need to be paid to the inclusion of legal and ethical concerns in the training and regulation of the profession, for instance through achieving greater familiarity with requirements of valuesensitive design [39] and increased collaboration with legal and ethical experts in the design and implementation process.

Another significant concern arises with regard to the digital divide which impacts on the practical usability of cloud robots due to socially unequal access to cloud services. While some healthcare robots are developed specifically for groups of digitally underserved users, such as older persons, the reliance on the cloud might prevent many of those users from availing of the technology. For example, domestic care robots might be particularly suitable for use in rural settings where isolation and access to care is a significant issue. However, those settings are, at least currently, exactly those which are frequently not yet served by reliable internet. Accordingly, specific social groups might systematically be excluded from these services. Taking account of such social factors needs to be part of strategic decision-making and the development process of specific robots.

IV. CONCLUSIONS

This paper has outlined that the currently envisaged use of cloud robotics in healthcare requires careful consideration of a range of legal and ethical issues in order to ensure a practice that is legally, ethically and socially acceptable. The emerging area of cloud robotics deserves to attract more attention from legal scholars and ethicists to enable recognition of cloud-related concerns as essential for the value sensitive design, use and implementation of new generations of robots in healthcare.
Policymakers should pay close attention to the questions arising with regard to the use of cloud resources in healthcare robotics due to the complexity of the technology and the vulnerability of many of the envisaged user groups. Action will be required especially by policymakers to create and clarify regulatory requirements to meet those challenges, ensure meaningful regulatory compliance, while respecting societal values and realizing user protection.

V. ACKNOWLEDGEMENTS

This research was partly funded by: EU Horizon 2020 Project MARIO “Managing active and healthy aging with use of caring service robots” (grant agreement 643808); The SIGNAL project at the University of Oslo; and the Cloud Legal Project at the Centre for Commercial Law Studies, Queen Mary University of London. E. Fosch-Villaronga is grateful to Microsoft for the generous financial support that has made this project possible. Responsibility for the views expressed, however, remains with the authors.

REFERENCES

[27] European Union (2016, July) Guide to the EU-U.S. Privacy Shield