Cybersecurity, value sensing robots for LGBTIQ+ elderly, and the need for revised codes of conduct

Adam Poulsen
Charles Sturt University
Australia
apoulsen@csu.edu.au

Eduard Fosch-Villaronga
Leiden Law School
Leiden University
The Netherlands

Oliver K Burmeister
Charles Sturt University
Australia

Abstract

Until now, each profession has developed their professional codes of conduct independently. However, the use of robots and artificial intelligence is blurring professional delineations: aged care nurses work with lifting robots, tablet computers, and intelligent diagnostic systems, and health information system designers work with clinical teams. While robots assist the medical staff in extending the professional service they provide, it is not clear how professions adhere and adapt to the new reality. In this article, we reflect on how the insertion of robots may shape codes of conduct, in particular with regards to cybersecurity. We do so by focusing on the use of social robots for helping LGBTIQ+ elderly cope with loneliness and depression. Using robots in such a delicate domain of application changes how care is delivered, as now alongside the caregiver, there is a cyber-physical health information system that can learn from experience and act autonomously. Our contribution stresses the importance of including cybersecurity considerations in codes of conduct for both robot developers and caregivers as it is the human and not the machine which is responsible for ensuring the system's security and the user's safety.

Keywords: aged care, AI, ethics, LGBTIQ+, healthcare robots, responsibility, value sensitive design.

1 Introduction

The use of robots and artificial intelligence (AI) is blurring professional delineations: aged care nurses work with lifting robots, tablet computers, and intelligent diagnostic systems, and health information system designers work with clinical teams. While robots assist the medical staff in extending the professional service they provide and robotics professionals are having closer interactions with the healthcare environment, it is not clear how professions adhere and adapt to the new reality. Professional codes of conduct developed in isolation fail to recognise the interplay of systems, stakeholders, and values. Since technologies are not value-neutral, they shape values and values shape them back and, in turn, these change the way we conceive the world, a cyber-attack to these technologies could have disastrous consequences for the user and alter the effectiveness of the task performed by the robot.

Security vulnerabilities in robots raise significant concerns for manufacturers and programmers, but especially for those who interact with them in a sensitive domain of application such as healthcare. If an attacker can compromise the controlling of the machines or have effects on the production chain (Quarta et al., 2017), any malfunctioning or any cybersecurity attack to a healthcare robot may affect the health, wellbeing, and safety of people, something that agencies like the Food and Drug Administration (FDA) in the U.S. identify as an unresolved, primary concern (FDA, 2019).

In an aged care setting where robots interact in close, direct contact with the elderly, any malfunctioning can result in a disastrous outcome. AI in medicine may improve, for instance, diagnoses made by humans (Razzaki et al., 2018), but they may have an over-focus on data and disregard the context, dismissing the value of ambiguity in observed phenomena. Missing these aspects could challenge, in turn, the correctness of the decision that might affect the wellbeing of the person. Since cybercrime operates at the speed of light and traditional law enforcement efforts operate at a much lower rate, questions about prevention and remedies, including distribution of responsibility in highly autonomous environments (Johnson, 2015), abound when we use and develop technology that may have a direct impact on a person’s wellbeing (Datteri, 2013; Fosch-Villaronga, 2019).

The delicacy of the domain of application, and the potential negative consequences these technologies could have demands for a multi-layered governance strategy that might take various forms, including guidelines, policies, standards, or codes of conduct. In this article, we argue that including cybersecurity considerations in codes of conduct for both robot developers and caregivers is imperative and of vital importance, as it is the human and not the machine which is responsible for ensuring the system's security and the user's safety (Pasquale, 2017). Still, although much work has gone into attempts to create universal codes of conduct (Al-Saggaf, Burmeister, & Schwartz, 2017; Burmeister, 2013, 2017; Capurro & Britz, 2010), more work is needed to understand how those principles affect the work of designers and developers of AI-driven healthcare robots.

Health information systems (IS) are not value-neutral and can have positive and negative impacts on the values within and arising from the ecosystem where these technologies are implemented (Legassick and Harding, 2017; Friedman & Hendry, 2019). To identify the implications for cybersecurity in codes of conduct for healthcare AI and robots, we examine data from an LGBTIQ+ elderly and care robot study. Using value sensitive design (VSD), we demonstrate how cyberattacks affect the diversity of values and value interpretations. We stress that current codes of conduct need to be revised to account for the diversity of values. Our contribution seeks to show how cybersecurity vulnerabilities of healthcare robot technologies affect users' values, and highlight the critical role and responsibility designers and developers have to ensure the user's overall safety, not only the system's security. Furthermore, this work shows how codes of conduct should be revised given the impacts of healthcare robot vulnerabilities on users’ values in the cyber and physical world.

2 Literature Review

A recent literature review sheds light on the contributions made to health IS by robotic care (Miah, Shen, Lamp, Kerr, & Gammack, 2019). This multidisciplinary research involves numerous forms of information processing to improve data acquisition, retrieving, analysing, processing, displaying, and using the information in health decision making. Their literature analysis showed that, concerning healthcare, workforce challenges (as seen particularly in aged care) are increasingly leading to innovative technological solutions, including robotic and AI-driven care.

Robotics have increased productivity and resource efficiency in the industrial and retail sectors, and now there is an emerging interest in realizing a comparable transformation in other areas, including healthcare (Cresswell, Cunningham-Burley, & Sheikh, 2018). However, a healthcare system delivered by or with the help of robots is not straightforward and raises many questions. These questions range from how safe robotized care is (Pino, Boulay, Jouen, & Rigaud, 2015; Fosch-Villaronga, 2019), how these robots enhance or diminish the dignity of users (Sharkey, 2014; Zardiashvili & Fosch-Villaronga, 2020), as to how the work of practitioners change in light of these new robotic systems (Melkas, Hennala, Pekkarinen, & Kyrki, 2020). Indeed, inserting robots in healthcare affects the whole ecosystem, which includes primary (direct robot users, clinicians, caregivers), secondary (robot makers, environmental service workers, health administrators), and tertiary stakeholders (policymakers, insurers, and advocacy groups). In this contribution, we focus on how robot makers' codes of conduct should be revised in light of the impacts healthcare robots' vulnerabilities have on users' values.

2.1 Cyberattacks and vulnerabilities of healthcare robots

Cybersecurity addresses protection from external, unintended penetration, or malicious disruption, and aims to safeguard the confidentiality, integrity, and availability of IS (Thomas, Burmeister, & Low, 2019). Cyberattacks on robotic and AI-driven technologies allow the materialization of attacks that go beyond the cyber world, and this deserves special attention in healthcare settings because "vulnerabilities could allow unauthorized users to remotely access, control, and issue commands to compromised devices, potentially leading to patient harm" (FDA, 2019). The remote hacking into a robot may be used to confuse or even attack a patient, steal the identity of a doctor, or to induce undesirable behaviours from the patient (Clark, Doran, & Andel, 2017). A malicious virus delivered using social engineering could manipulate the output from a diagnosis decision support tool. Moreover, the use of backdoors in outdated operating systems of robots or medical devices might allow the stealing of sensitive information about the patient (Coronado and Wong, 2014).

Patient-centred healthcare culture may sometimes undermine the importance of security, although ISs dominate the healthcare system. Password sharing amongst healthcare workers is an example of this culture, challenging the security of the systems and the privacy of users (Martin, Martin, Hankin, Darzi, & Kinross, 2017). Since any system connected to the Internet is subject to cyberattacks, however, the continuous use of cyber-physical systems in the healthcare sector demands robust cybersecurity mechanisms that can ultimately ensure patients' safety. Moreover, the growing interconnectivity and integration of healthcare technologies open multiple points of entry for cyberattacks, providing attackers with remote access to various interconnected systems from one access point, allowing attacks to go often unnoticed. Cyberattacks on interconnected systems (with a denial of service attack, for instance) can harm a healthcare facility by disrupting the operation of networked medical devices and the integrity of information (Coronado and Wong, 2014).

The possibility to extend home care via care robots further exacerbates this panorama. Users usually fail to recognize that the robot is not the only relevant unit in the ecosystem, but that other information flows happen in the background (Fosch-Villaronga, Felzmann, Ramos-

Montero, & Mahler, 2018; Fosch-Villaronga and Millard, 2019). Coupled with the strong industry push for the development of trustworthy robots and AI systems (HLEG AI, 2019; Floridi, 2019), the little knowledge on the overall functioning of the robot calls for more than just a precautionary approach when it comes to cybersecurity.

2.2 Caring for LGBTIQ+ elderly

Culture shapes a person's value system; one of the most significant influences on an individual's values is each person's cultural background (Drayton & Weston, 2015; Horton, Tschudin, & Forget, 2007; Huang, Teo, Sánchez-Prieto, García-Peñalvo, & Olmos-Migueláñez, 2019; Liu, Volcic, & Gallois, 2014; Sunny, Patrick, & Rob, 2019). Tenenbaum (2011) describes the LGBTIQ+ community as a culture with unique values, concerns, needs, and critical and experiential interests in healthcare. Many LGBTIQ+ persons explicitly seek out services that are LGBTIQ-friendly and healthcare professionals who are sensitive to the needs and values of their community (Jann, Edmiston, & Ehrenfeld, 2015).

The use of social robots could help members of this community cope with loneliness and depression in the same way they have benefited the broader ageing population (Birks, Bodak, Barlas, Harwood, & Pether, 2016; Carter-Templeton, Frazier, Wu, & H. Wyatt, 2018; Khosla et al., 2012; Moyle, Jones, & Sung, 2020). However, system vulnerabilities may lead to just the opposite. A man-in-the-middle attack or an SQL injection that captures health data could reveal LGBTIQ+ elders undisclosed gender identity or sexual orientation, which is considered sensitive data in most privacy regulations. Wardriving could expose and abuse weak or open Wi-Fi wireless networks in aged care facilities and access health records of LGBTIQ+ elders. Hijacking a companion robot could lead unintended users to vocalize offensive, anti-LGBTIQ+ language, which could seriously endanger the trust the user put into the system. A distributed denial-of-service attack on a networked telepresence robot set up to provide a social network for LGBTIQ+ elders experiencing loneliness could seriously increase social isolation.

2.3 Codes of conduct for a robotized healthcare

Despite codes of professional conduct that ensure workers respect the welfare of and sensitivity to LGBTIQ+ persons, experiences of professional care have not lived up to these (Bennett et al., 2017). This has led to this group being "significantly more likely to delay or avoid necessary medical care compared with heterosexuals" (29% versus 17%, respectively) (Khalili, Leung, & Diamant, 2015). Whether the inclusion of robots would change this panorama is a question that remains unanswered.

Considering the complexity and the potential implications of robot technologies, the European Parliament proposed in 2017 a code of conduct for robotics engineers (European Parliament, 2017). The ethical code was an all-embracing sector framework directed towards realizing the development of robot technologies in compliance with European law. The framework included the principles of bioethics, mainly beneficence, non-maleficence, autonomy, and justice, and also the need to respect the dignity, privacy, and safety of humans (European Parliament, 2017). The Parliament stressed the importance of considering humans and not robots as responsible agents to comply with fundamental rights, work with precaution and inclusiveness, maximize benefit, and minimize harm. This human-centred responsibility is shared among scholars (Bryson, Diamantis, & Grant, 2017; Floridi et al., 2018) and also among the AI principles charts and governance documents around the world (Fjeld et al., 2019).

Fjeld et al. (2019) conclude that the majority of ethical and rights-based approaches in the governance of AI focus on the protection of human rights, promotion of human values, professional responsibility, human control of technology, fairness and non-discrimination, transparency and explainability, safety and security, accountability, and privacy. However, while the AI principle of *professional responsibility* appears to be most prominent in Google (Google, 2019), and to some degree in other organizations like Tesla, ITI, University of Montreal, IEEE, Future of Life Institute, Global Network Initiative, Smart Dubai, and the European High-Level Expert Group on AI, the principle it does not appear in the AI Principles of Telefonica, Microsoft AI Principles, the SAGE Ethics of Code, the European Ethical Charter on the use of AI in Judicial Systems, Seeking Ground Rules for AI, the Principles to Promote FEAT AI in the Financial Sector, AI in the UK, AI for Europe, AI at the Service of Citizens (Italy), White Paper on AI Standardization (China), Preparing for the future of AI (US NSTC), and the Think20 future of work and education for the digital age (Field et al., 2019).

A lack of professional responsibility coupled with a continuous focus on trustworthy AI (HLEG AI, 2019) risks diminishing scrutiny of professionals and undermines certain societal obligations of AI producers, shifting accountability further towards AI systems and away from professionals (Jobin, Ienca, & Vayena, 2019). Global governance charts focus more on the principle of non-maleficence rather than beneficence, appearing that "issuers of guidelines are preoccupied with the moral obligation to prevent harm" instead of promoting those values (Jobin, Ienca, & Vayena, 2019). In this sense, the importance of having professional codes of conduct that ground the work of robot makers in respect of fundamental rights becomes paramount.

3 Methods

The present constructivist study is a part of a larger project which aims to improve LGBTIQ+ aged care through the use of care robots. The project suggests the use of value sensing robots to make person-centred, value-driven decisions in situ, as limited by a framework guaranteeing duty of care, professional ethics, and law.

Thirty-two people were interviewed about aged care, social robots, and loneliness. We followed a purposive sample that included healthcare and LGBTIQ+ service provider professionals, robot designers, and seventeen Australian LGBTIQ+ elders (65+) (twelve gay men, two lesbian women, one gay gender-fluid person, one lesbian non-binary person, and one bisexual non-binary person). Only the interviews of the seventeen Australian LGBTIQ+ elders are analysed here. Interview length was determined by each participant, the shortest was thirty minutes and the longest was one hour and forty minutes. Participants were located in rural and metropolitan New South Wales and Victoria, as well as metropolitan South Australia and Queensland.

Through semi-structured interviews, participants were questioned about the LGBTIQ+ experience of aging, aged care, social isolation, and loneliness, as well as the older LGBTIQ+ community's values. The interviews were transcribed and analysed using thematic analysis with QSR NVivo 12, a software package for managing qualitative data. The lead investigator analysed all interviews. A selection of the interviews was also analysed independently by another investigator for inter-rater reliability, with the two investigators discussing discrepancies in analysis, to ensure the reliability of interpretation of the results. Ethics approval from the university and from participating LGBTIQ+ communities, from which participants were recruited for this and the more extensive study, was obtained.

The part of the study presented here focuses on the impressions of users concerning social robots and loneliness, with a particular focus on cybersecurity aspects. The findings in the next section have implications for codes of conduct for AI-driven and robotic healthcare systems.

4 Findings

Four themes emerged from the analysis of the interviews. They were privacy, safe systems, internet connectivity, and determinants of security for LGBTIQ+ elders, see Table 1 below. Exemplary quotations addressing cybersecurity considerations are explored below.

Themes	Categories
Privacy	Dignity Choice Historical and contemporary discrimination
Safe systems	Safety Safe physical locations Emergency help with robots
Internet connectivity	Robots disconnected from the Internet Online scams Trust
Determinants of security for LGBTIQ+ elders	Appreciating difference LGBTIQ+ connectivity & community Not tolerance, acceptance LGBTIQ-friendly service provision

Table 1. Themes and the categories of the interviews about aged care, social robots, and loneliness

4.1 Theme 1: Privacy

Several participants expressed concerns for choice and dignity regarding privacy:

> *Can you turn it off, like sometimes you just feel like not talking to anybody and just go I'm not interested. (67, gay gender-fluid person)*

> *Where having a monitor and somebody observing you and you can talk to and they can move the thing around the house to make sure … it takes away a certain amount of privacy … probably your dignity, because you could be there terrified to do anything, because who's watching me? (68, gay man)*

Other privacy concerns directly related to being LGBTIQ+ and historical and contemporary discrimination also emerged.

> *That's what shut me off about the equal marriage plebiscite. I just felt, I thought it was so rude to ask straight people to say whether they thought it was okay for me and my friends to get married. It had nothing to do with them. (65-70, gay man)*

> *You watched the way you walked, you watched the way you spoke, you didn't want anyone to realize your secret. And my family, I didn't come out to my family until I was 42 and I was*

> *dying, I only came out to them because everyone thought I was about to die so we had to tell mom and dad. So, it was just, the secrecy was just terrible. (66, gay man)*

Many participants expressed fears of discrimination and highly prioritized privacy. There are existing processes in healthcare, such as an open-door policy that allows healthcare professionals to enter a person's private room with little warning, perpetuating a system in which privacy is lacking. The introduction of healthcare robots may also remove choice and lack historical awareness of the LGBTIQ+ experience, creating a fear of discrimination and heightening the need for privacy.

4.2 Theme 2: Safe systems

Common concerns among participants for safety and safe physical locations are seen in the following exemplary quotations.

> *We value highly how to keep ourselves safe. You know, I guess that's a no brainer. Because I know people who have died. I know people who have been seriously brutalized by police. You know, that's not good. But we value security if we can find it. (65, lesbian nonbinary)*

> *It's just sometimes I said to myself, "Go back into the closet, [name], hide. That will keep you safe. Let people think whatever they want to think." (65, lesbian nonbinary)*

Emergency help with robots was another category identified. Multiple participants noted the practical advantages of having a robot which could aid in calling for emergency help.

> *Being the manager of the village, you have a key to everybody's unit – well, master key to everybody's unit so to get in in emergency situations. We got in and the neighbour came with me and I said, "Just stay with me but behind me." We found the lady on the kitchen floor, she had been there for nearly 12 hours … So, one of the things I would like to see included in your robot thing is if that particular person does have a fall, the robot can set off the alarm … That would be a very good thing to have, particularly people who are single and live alone. (68, gay man)*

4.3 Theme 3: Internet connectivity

Internet connectivity was a contentious issue. Some participants noted the usefulness of having a system which is connected to the Internet to help connect them to others. However, as highlighted here, some participants were troubled by the idea of having robots in their home and connected to the Internet for fear of hacking and having information stolen or having interactions with the robot influenced by a hacker.

> *Have to be through somebody like some sort of maybe Aged Care organization that can come and install them, you know what I mean? ... Like the internet, some people can, you know, you hack into those and people can do some terrible things. (70, gay man)*

> *If you get the artificial intelligence to work not link to the net … It's having the conversation and the internet not knowing where it's going to end up, or where its security is. If you can write is so that its security is something that we feel comfortable with or I feel comfortable with, then I will engage with it. If I'm worried that that conversation is going to be polluted some way into, then I would be very wary. (66, Lesbian woman)*

One participant had been the victim of an online scam in the past.

> *I was scammed, would you believe it, not long after I got the laptop when I was searching for work and I was taken like hook line and sinker. Fortunately, I got the money that I put up front. I really was taken for a ride … you wouldn't want anything like that happening. (70, gay man)*

Trust was also identified as a category in the Internet connectivity theme. That is, trust in other persons online.

> *Having a conversation with a robot is fine … What I would like is a chat machine that you can trust as opposed to the internet where you don't… I wouldn't trust chatting on the internet. (66, lesbian woman)*

Trust also came up in relation to LGBTIQ+ elders with no family or partner, such as the potential of having to trust someone with handling their finances. This concern might be applied to the cybersecurity of healthcare systems, i.e. having to place trust in a virtual or robotic assistant helping with online banking.

> *Look at the LGBT elders, for instance, like myself, that's not a relationship, that has family that are on the other side of Sydney. Yes, I am alone. I have concerns about my life in the future, about if I got short term memory issues, who is going to do my banking that I can trust? Who's going to make sure I've got food in the house, all those sorts of things? (65-70, gay man)*

4.4 Theme 4: Determinants of security for LGBTIQ+ elders

This theme captures the narrative about the older LGBTIQ+ community's determinants of a feeling of security. Understanding these determinants of security creates knowledge about what LGBTIQ+ elders need from robotic and AI systems regarding cybersecurity. Appreciating difference refers to how several participants in this study voiced the notion of inclusivity.

> *People to be able to appreciate that you are different but you're still a human being. (67, gay gender-fluid person)*

> *I think we have to be inclusive in our caring for the elderly. And also, from whether it's gay or whether it's from ethnic backgrounds, you have to be inclusive as well. (68, gay man)*

> *We value inclusion … people sort of go back into their own, you know, the gay holes, the lesbian holes, the trans holes … the community is ghettoized and difficult to get to. And there's a reason for that, and that is because the community, as in the various sections of the community have to put up walls when we're not coming together as a group like that, to protect ourselves. (65, lesbian nonbinary)*

LGBTIQ+ connectivity and community were sought out by some LGBTIQ+ elders in this study, but not all. Some participants wanted to be exclusively surrounded by the LGBTIQ+ community for a sense of security and connection. Whereas others for community and connectivity reasons, not for security, valued diverse friendships and connections outside of the LGBTIQ+ community, and the remaining few participants did not want to be connected to the LGBTIQ+ community. Those who did seek out LGBTIQ+ connectivity and community for a sense of security are highlighted here.

> *I have run across quite a few gays in [place] – as far as the gay men's social group are concerned there are quite a lot of older guys. One of the oldest one in our group is 82 but he still lives at home on his own and he's very active … we do rely on each other. And one of the reasons I'm*

> *part of that group is that if anybody gets really sick that we can all support each other and help if we need to. (68, gay man)*

> *I used to do a lot of work in the gay community. And I still have a lot of friends my age, who are very community-minded and happy to usually answer questions. (65-70, gay man)*

> *The notion of family is very, very strong within the community, the value of sticking together and being together because we need each other for protection … I'd say one of the most powerful values that the community has is a sense of community, that we are a community of people. And you know, I mean, I don't hesitate when I'm around my community, I relax, my guard goes down. And I think we saw it during the same sex marriage thing. Another powerful value that we have is that our lives are about love and caring … sure we can get a bit of antipathy happening across the gay/lesbian divide. And also of course, obviously trans, a lot of trans people get a very bad time within the community. So, yeah, there are, because trans are the most reviled and hated by the straight world and also misunderstood within the community. (65, lesbian nonbinary)*

Tolerance does not instil a sense of security, whereas acceptance does.

> *Acceptance is a very key value, not tolerance, acceptance. Because of course, we all deal with our own families and sometimes it's a big deal for people to come out to the straight world. (65, lesbian nonbinary)*

The last category identified in the determinants of security for LGBTIQ+ elders theme, was LGBTIQ-friendly service provision.

> *My home may become quite a dangerous place for me if services that I access are antagonistic. So, it's a big, big issue, really big … being already a marginalized group of people, as we get older, we need more advocacy. (65, lesbian nonbinary)*

> *I've been invited to speak to a couple of age care or age-related conferences on LGBTI aging and the issues of practitioners you have to be aware of because the queer aging population has had a very different life course from those who are young and serving them now in healthcare centres or hospitals or doctor's surgeries or whatever. (72, gay man)*

5 Discussion

The findings have implications for cybersecurity in codes of conduct. Healthcare professionals and designers of health IS need to be aware of the historical queer experience and bring that awareness into care delivery (Shields & Burmeister, 2018). Their codes of conduct need to prioritize privacy and safe physical locations in which unwanted surveillance does not occur, nor the theft of personal information. LGBTIQ+ elders arguably feel even more vulnerable than their heterosexual peers about hackers uncovering and revealing a person's gender identity or sexual orientation. This feeling and potential cybersecurity threat might be increased by the introduction of healthcare robots in one's home.

Values in motion design (VMD) seeks to create AI where value sensing robots make explicit value-driven decisions to govern actions; these decisions are shaped to the values of the user and user community in situ when it is safe to do so as governed by a framework guaranteeing duty of care, professional ethics, and law which is embedded into the design of the robot (Poulsen & Burmeister, 2019). Care robot designers creating value sensing robots ought to develop a basic care robot framework based on values found in applied ethics, such as professional ethics and law, thereafter they should investigate individual and community-based values that the care robot can then shape to the individual during run-time to provide person-centred care. The guiding principle of VMD is the ability to distinguish between intrinsic (pre-programmed) and instrumental care (in-situ) values. This distinction is grounded in applied ethics (e.g., intrinsic values emerging from professional ethics and codes, healthcare law, robot design standards, and duty of care) and descriptive ethics (e.g., instrumental values emerging from determinative in practice, person-centred, culturally competent care), respectively. Furthermore, care robot designers should make intrinsic and preliminary instrumental value decisions, and value sensing robots are to make effective value decisions in relationship with the user by adapting and building off of those initial instrumental value decisions within the limits set out by those intrinsic ones.

Consider the following scenario in Table 2:

Scenario for cybersecurity implications for LGBTIQ+ users
An LGBTIQ+ elder uses a telepresence care robot to video call healthcare professionals and friends from their home. The hacker performs a man-in-the-middle attack to intercept video data and learns of their closeted sexual orientation. The hacker then attempts to make a video call to the user with the intention of blackmailing the LGBTIQ+ elder with that sensitive information.

Table 2. Scenario for cybersecurity implications for LGBTIQ+ users

The implications of a cyberattack can be disastrous. Healthcare professionals' code of conduct ensured confidentiality. However, inserting a robot challenges how cyber-physical systems ensure confidentiality. These concerns ought to be accounted for in codes of conduct, both in robot developers' codes of conduct and in caregivers as well.

In principle, value sensing robots could attempt to make use of instrumental values to achieve intrinsic ones better. A value sensing robot could shape the way it achieves cybersecurity by taking into account the values of the individual user and the user community, in situ (Poulsen, Burmeister, & Kreps, 2018; Poulsen, Skaines, Mclaren, & Burmeister, 2020). Considering the scenario in Table 2, a value sensing robot might be able to help because, contrary to other robots that do not account for values in situ, the value sensing robot has ascertained that the user, like many LGBTIQ+ elders, is concerned with trust regarding Internet-connected robot systems through its previous interactions with the LGBTIQ+ elder user. Accordingly, the robot accounts for the user's trust and allows only trusted contacts to initiate a call with the user. The robot would check incoming calls using facial recognition and would be able to adapt its behaviour if a non-trusted contact is calling. The hacker's incoming call would be prevented because third parties cannot initiate contact with the LGBTIQ+ elder. By adapting its behaviour and accounting for the instrumental value of trust in this way, the value sensing robot better accomplishes cybersecurity in the scenario and meets the requirement of adapting to the changing needs of users.

Adherence to a particular design methodology, such as value sensitive design (Friedman, Kahn, & Borning, 2006; Friedman & Hendry, 2019; Poulsen & Burmeister, 2019) or user-centred design, could help address cybersecurity and user safety considerations (Denning et al., 2014; Tanev, Tzolov, & Apiafi, 2015; Henschke & Ford, 2017). Although there is no concrete binding law that establishes a safeguard baseline for healthcare robots to be respected by those who design these technologies, unfortunately (Fosch-Villaronga, 2017; Poulsen, Burmeister, & Tien, 2018), professional codes are an excellent mechanism to actuate juridical principles. Indeed, although existing laws can better inform healthcare technology design decisions when following these methods, inserting these methodologies in professional codes of conduct could be more efficient in making the work of developers account for user's values. An example is the United Kingdom Department of Health & Social Care (2019) released a Code for data-driven health and care technology. The idea behind it was to 'enable the development and adoption of safe, ethical, and effective data-driven health and care technologies.' Its principle nine promoted the integration of security and data protection into the design of the technology and released a toolkit to ease its implementation.

The code of conduct of the UK seems a mere compliance guideline, nonetheless with Art. 25 of the General Data Protection Regulation, which focuses on privacy by design and by default (GDPR, 2018). However, these are not the only values involved in care practices, at least not for LGBTIQ+ elders. The literature suggests that LGBTIQ+ elders prioritize values of acceptance, privacy, and personhood (Tenenbaum, 2011); inclusive language and normalization of disclosing gender identity or sexual orientation (Huygen, 2006); autonomy and empowerment (Waite, 2015); and non-judgemental care (Latham and Barrett, 2015). LGBTIQ+ elders also define values uniquely (Waling & Roffee, 2017). Not accounting for all these values would disregard the LGBTIQ+ community values and perpetuate discrimination against the queer community (Poulsen, Fosch-Villaronga, & Søraa, 2020; Gomes, Antonialli, & Dias-Oliva, 2019).

The GDPR is also a corpus that mostly misses the cyber-physical nature of robots and embodied AI (Fosch-Villaronga and Millard, 2019). AI and robotic technologies are not mere data-driven technologies and do not only challenge data protection. In this respect, a code of conduct for professionals working on AI and robotics should take into consideration how the embodiment of such technologies plays a role in the overall interplay between user interaction and the protection of fundamental rights. Moreover, it should take into account the whole ecosystem surrounding these technologies, which includes the manufacturer of the physical robot, the operating system, firmware, software, mobile/remote control applications; the vendor of internet, cloud services, and networks; and the professionals working with it, including the hospital or the direct caregivers and the care-receivers.

6 Conclusion

More research is needed in areas such as the governance of cybersecurity for AI-driven, and robotic healthcare IS. These systems have a dual cyber-physical nature, the capacity to learn from experience and act autonomously. These capabilities demand the careful attention of those working on the design and development of such systems with vulnerable populations. In our work, we identified four categoric concerns implicated in the cybersecurity of AI-driven and robotic healthcare IS for the older LGBTIQ+ community: 1) privacy, 2) safety, 3) internet connectivity, and 4) determinants of security for LGBTIQ+ elders.

Cybersecurity in the design, development, and use of AI-driven robot healthcare technologies often goes ungoverned, although it may affect users' values. Codes of conduct need to reflect such end-user concerns so that robot-human interaction design meets their requirements. Currently, such codes reflect the individual responsibilities of IS professionals (Burmeister, 2017; Burmeister, Thomas, & Poulsen, 2018), but they need to be extended to include the evolution of their products, beyond the initial implementation stages, such as for dynamically changing online platforms, and for value sensing robots which adapt care to the changing needs of their users (Poulsen & Burmeister, 2019). That adaptation ability also needs to be the subject of codes of conduct and, ultimately, the law.

It is imperative that robot developers understand the magnitude and scale of cybersecurity implications for users in particular and society at large and that caregivers understand that including robots for care delivery is not straightforward (Fosch-Villaronga, 2019). Our study indicates the importance of including cybersecurity considerations in codes of conduct as it is the human and not the machine which is responsible for ensuring the system's security.

Acknowledgment

Part of this project was funded by the LEaDing Fellows Marie Curie COFUND fellowship, a project that has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement no. 707404.

References

Al-Saggaf, Y., Burmeister, O. K., & Schwartz, M. (2017). Qualifications and ethics education: the views of ICT professionals. *Australasian Journal of Information Systems, 21*

Bennett, E., Berry, K., Emeto, T. I., Burmeister, O. K., Young, J., & Shields, L. (2017). Attitudes to lesbian, gay, bisexual and transgender parents seeking health care for their children in two early parenting services in Australia. *Journal of Clinical Nursing, 26*(7-8), 1021–1030. doi:10.1111/jocn.13595

Birks, M., Bodak, M., Barlas, J., Harwood, J., & Pether, M. (2016). Robotic seals as therapeutic tools in an aged care facility: A qualitative study. *Journal of Ageing Research, 2016*. doi:10.1155/2016/8569602

Bryson, J. J., Diamantis, M. E., & Grant, T. D. (2017). Of, for, and by the people: the legal lacuna of synthetic persons. *Artificial Intelligence and Law*, *25*(3), 273-291

Burmeister, O. K., Thomas, G., & Poulsen, A. (2018). Professional ethics involving cyber security and autonomous robots. In S. G. Tzafestas (Ed.), *Information, communication, and automation technology ethics in the knowledge society age*. Nova Science Publishers

Burmeister, O. K. (2017). Professional ethics in the information age. *Journal of Information, Communication and Ethics in Society*, 15(4), 348-356. doi:10.1108/JICES-11-2016-0045

Burmeister, O. K. (2013). Achieving the goal of a global computing code of ethics through an international-localisation hybrid. *Ethical Space: The International Journal of Communication Ethics, 10*(4), 25-32

Capurro, R., & Britz, J. B. (2010). In search of a code of global information ethics: The road travelled and new horizons. *Ethical Space: The International Journal of Communication Ethics, 7*(2/3), 28-36

Carter-Templeton, H., Frazier, R. M., Wu, L., & H. Wyatt, T. (2018). Robotics in nursing: A bibliometric analysis. *Journal of Nursing Scholarship, 50*(6), 582-589. doi:10.1111/jnu.12399

Clark, G. W., Doran, M. V., & Andel, T. R. (2017). Cybersecurity issues in robotics. Paper presented at the *2017 IEEE Conference on Cognitive and Computational Aspects of Situation Management* (CogSIMA)

Coronado, A. J., & Wong, T. L. (2014). Healthcare cybersecurity risk management: Keys to an effective plan. *Biomedical Instrumentation & Technology*, *48*(s1), 26-30

Cresswell, K., Cunningham-Burley, S., & Sheikh, A. (2018). Health care robotics: qualitative exploration of key challenges and future directions. *Journal of Medical Internet Research*, *20*(7), e10410

Datteri, E. (2013). Predicting the long-term effects of human-robot interaction: A reflection on responsibility in medical robotics. *Science and engineering ethics, 19*(1), 139-160

Denning, T., Kramer, D. B., Friedman, B., Reynolds, M. R., Gill, B., & Kohno, T. (2014). CPS: beyond usability: applying value sensitive design based methods to investigate domain characteristics for security for implantable cardiac devices. *Proceedings of the 30th Annual Computer Security Applications Conference*. New Orleans, Louisiana, USA. doi:10.1145/2664243.2664289

European Parliament (2017) *Resolution on Civil Law Rules on Robotics*. Retrieved from http://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html

Fjeld, J., Hilligoss, H., Achten, N., Levy Daniel, M., Feldman, J., Kagay, S. (2019) *Principled Artificial Intelligence*. Retrieved from https://cyber.harvard.edu/publication/2020/principled-ai

Floridi, L. (2019). Establishing the rules for building trustworthy AI. *Nature Machine Intelligence, 1*(6), 261-262

Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., ... & Schafer, B. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds and Machines*, *28*(4), 689-707

Food and Drug Administration, FDA (2019) *Cybersecurity*. Retrieved from https://www.fda.gov/medical-devices/digital-health/cybersecurity

Fosch Villaronga, E. (2017). *Towards a Legal and Ethical Framework for Personal Care Robots. Analysis of Person Carrier, Physical Assistant and Mobile Servant Robots.* (Doctoral dissertation, University of Bologna, Bologna, Italy)

Fosch-Villaronga, E. (2019). *Robots, healthcare, and the law: Regulating automation in personal care*. Routledge

Fosch-Villaronga, E., Felzmann, H., Ramos-Montero, M., & Mahler, T. (2018). Cloud services for robotic nurses? Assessing legal and ethical issues in the use of cloud services for healthcare robots. *Proceedings of 2018 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)* (290-296)

Fosch-Villaronga, E. and Millard, C. (2019). Cloud robotics law and regulation: Challenges in the governance of complex and dynamic cyber-physical ecosystems. *Robotics and Autonomous Systems 119,* 77-91. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3305353

Friedman, B., & Hendry, D. G. (2019). *Value Sensitive Design: Shaping Technology with Moral Imagination*: MIT Press

Friedman, B., Kahn, P. H. J., & Borning, A. (2006). Value sensitive design and information systems. In P. Zhang & D. Galletta (Eds.), *Human-Computer Interaction and Management Information Systems: Foundations* (pp. 348-372). New York: M. E. Sharpe

General Data Protection Regulation, GDPR (2018). Article 25 EU *General Data Protection Regulation.* Retrieved from https://www.privacy-regulation.eu/en/article-25-data-protection-by-design-and-by-default-GDPR.htm

Gomes, A., Antonialli, D. & Dias-Oliva, T. (2019) Drag queens and artificial intelligence. Should computers decide what is toxic on the internet? *Internet Lab blog*. Retrieved from http://www.internetlab.org.br/en/freedom-of-expression/drag-queens-and-artificial-intelligence-should-computers-decide-what-is-toxic-on-the-internet/

Henschke, A., & Ford, S. B. (2017). Cybersecurity, trustworthiness and resilient systems: guiding values for policy. *Journal of Cyber Policy, 2*(1), 82-95. doi:10.1080/23738871.2016.1243721

High-Level Expert Group on Artificial Intelligence, HLEG (2019). *Ethics Guidelines for Trustworthy AI*. Retrieved from https://ec.europa.eu/futurium/en/ai-alliance-consultation

Huygen, C. (2006). Understanding the needs of lesbian, gay, bisexual, and transgender people living with mental illness. *MedGenMed: Medscape General Medicine, 8*(2), 29-29. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1785208/

Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, *1*(9), 389-399

Johnson, D. G. (2015). Technology with no human responsibility?. *Journal of Business Ethics*, *127*(4), 707-715

Khosla, R., Chu, M.-T., Kachouie, R., Yamada, K., Yoshihiro, F., & Yamaguchi, T. (2012). Interactive multimodal social robot for improving quality of care of elderly in Australian nursing homes. *Proceedings of the 20th ACM International Conference on Multimedia*. doi:10.1145/2393347.2396411

Latham, J., & Barrett, C. (2015). Appropriate bodies and other damn lies: Intersex ageing and aged care. *Australasian Journal on Ageing, 34*(S2), 19-20. doi:10.1111/ajag.12275

Legassick, S., & Harding, V. (2017). *Why we launched DeepMind Ethics & Society*. Retrieved from https://deepmind.com/blog/announcements/why-we-launched-deepmind-ethics-society

Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: how safe are we?. *BMJ, 358*, j3179, 1-4

Melkas, H., Hennala, L., Pekkarinen, S., & Kyrki, V. (2020). Impacts of robot implementation on care personnel and clients in elderly-care institutions. *International Journal of Medical Informatics, 134*, 1-6. doi:10.1016/j.ijmedinf.2019.104041

Miah, S., Shen, J., Lamp, J. W., Kerr, D., & Gammack, J. (2019). Emerging insights of health informatics research: A literature analysis for outlining new themes. *Australasian Journal of Information Systems, 23*. doi:10.3127/ajis.v23i0.2137

Moyle, W., Jones, C., & Sung, B. (2020). Telepresence robots: Encouraging interactive communication between family carers and people with dementia. *Australasian Journal on Ageing, 39*(1), 127-133. doi:10.1111/ajag.12713

Pasquale, F. (2017). Toward a fourth law of robotics: Preserving attribution, responsibility, and explainability in an algorithmic society. *Ohio State Law Journal, 78*. Retrieved from https://ssrn.com/abstract=3002546

Pino, M., Boulay, M., Jouen, F., & Rigaud, A. S. (2015). "Are we ready for robots that care for us?" Attitudes and opinions of older adults toward socially assistive robots. *Frontiers in Aging Neuroscience*, *7*, 141, doi:10.3389/fnagi.2015.00141

Poulsen, A., Skaines, I., Mclaren, S., & Burmeister, O. (2020). Value sensing robots: The older LGBTIQ+ community. *Proceedings of the 18th International Conference on the Ethical and Social Impacts of ICT (ETHICOMP)*

Poulsen, A., & Burmeister, O. K. (2019). Overcoming carer shortages with care robots: Dynamic value trade-offs in run-time. *Australasian Journal of Information Systems, 23*. doi:10.3127/ajis.v23i0.1688

Poulsen, A., Burmeister, O. K., & Kreps, D. (2018). The ethics of inherent trust in care robots for the elderly. In D. Kreps, C. Ess, L. Leenen, & K. Kimppa (Eds.), *This Changes Everything – ICT and Climate Change: What Can We Do?* (pp. 314-328). doi:10.1007/978-3-319-99605-9_24

Poulsen, A., Burmeister, O. K., & Tien, D. (2018). A new design approach and framework for elderly care robots. *Proceedings of the Australasian Conference on Information Systems.* Retrieved from http://www.acis2018.org/wp-content/uploads/2018/11/ACIS2018_paper_162.pdf

Poulsen, A., Fosch-Villaronga, E., & Søraa, R. A. (2020). Queering machines. *Nature Machine Intelligence, 2*, 152. doi:10.1038/s42256-020-0157-6

Quarta, D., Pogliani, M., Polino, M., Maggi, F., Zanchettin, A. M., & Zanero, S. (2017). An experimental security analysis of an industrial robot controller. *Proceedings of 2017 IEEE Symposium on Security and Privacy (SP)* (pp. 268-286)

Razzaki, S., Baker, A., Perov, Y., Middleton, K., Baxter, J., Mullarkey, D., ... & DoRosario, A. (2018). A comparative study of artificial intelligence and human doctors for the purpose of triage and diagnosis. *arXiv preprint arXiv:1806.10698*

Sharkey, A. (2014). Robots and human dignity: A consideration of the effects of robot care on the dignity of older people. *Ethics and Information Technology*, *16*(1), 63-75

Shields, L., & Burmeister, O. (2018). Education needed to enhance inclusive, non-discriminatory nursing practice towards lesbian, gay and bisexual parents. *Evidence Based Nursing, 21*(2), 47. doi:10.1136/eb-2017-102853

Tanev, G., Tzolov, P., & Apiafi, R. (2015). A value blueprint approach to cybersecurity in networked medical devices. *Technology Innovation Management Review, 5*(6). Retrieved from http://timreview.ca/article/903

Tenenbaum, E. M. (2011). Sexual expression and intimacy between nursing home residents with dementia: Balancing the current interests and prior values of heterosexual and LGBT residents. *Temple Political & Civil Rights Law Review, 21,* 459

Thomas, G., Burmeister, O., & Low, G. (2019). The importance of ethical conduct by penetration testers in the age of breach disclosure laws. *Australasian Journal of Information Systems*, 23. doi:10.3127/ajis.v23i0.1867

United Kingdom Department of Health & Social Care. (2019). *Code of conduct for data-driven health and care technology*. Retrieved from https://www.gov.uk/government/publications/code-of-conduct-for-data-driven-health-and-care-technology/initial-code-of-conduct-for-data-driven-health-and-care-technology

Waite, H. (2015). Old lesbians: Gendered histories and persistent challenges. *Australasian Journal on Ageing, 34*(S2), 8-13. doi:10.1111/ajag.12272

Waling, A., & Roffee, J. A. (2017). Knowing, performing and holding queerness: LGBTIQ+ student experiences in Australian tertiary education. *Sex Education, 17*(3), 302-318. doi:10.1080/14681811.2017.1294535

Zardiashvili, L., & Fosch-Villaronga, E. (2020). "Oh, dignity too?" Said the robot: Human dignity as the basis for the governance of robotics. *Minds and Machines*, 1-23

doi: https://doi.org/10.3127/ajis.v24i0.2789