様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　３ 年　 ６ 月 ２４ 日現在

機関番号：１１３０１
研究種目：若手研究
研究期間：2019～2020
課題番号：１９Ｋ１３５７９

研究課題名（和文）Data Protection in Human-Robot Interaction: A Focus on Healthcare Robots

研究課題名（英文）Data Protection in Human-Robot Interaction: A Focus on Healthcare Robots

研究代表者
翁　岳暄（Weng, Yueh-Hsuan）

東北大学・学際科学フロンティア研究所・助教

研究者番号：４０８１０８９１

交付決定額（研究期間全体）：（直接経費）　　2,400,000円

研究成果の概要（和文）：このプロジェクトの目的は、知能ロボットの身体性が、現在のデータ駆動型のプライバシー法規制にどのように影響するかを理解することです。 本研究は、理論的分析、HRI for Legal Validation実証実験との 2 つの主要な部分で構成されています。研究成果は、ケンブリッジ ハンドブック、IEEE国際会議論文、スタンフォード ワーキング ペーパーで公開されています。

研究成果の学術的意義や社会的意義
The embodiment characteristics of healthcare robots allows new possibilities for human-robot interaction (HRI). This impacts their relationship with the law. Among them, the legal concern on privacy and data protection associated with embodiment in HRI is the main focus of this research project.

研究成果の概要（英文）：The objective of this project is to understand how intelligent robots' characteristics of "embodiment" influence current data-driven privacy regulations. It includes two main parts as theoretical review, and HRI experiments. Research outputs have been published at the Cambridge Handbook, IEEE Conference Paper and Stanford Working Paper.

研究分野：新領域法学

キーワード：Data Protection　Human-Robot Interaction　Robot Law　Privacy by Design　AI Ethics

１．研究開始当初の背景

Developments in the embodied versions of systems operating with algorithms have brought about new possibilities for human-robot interaction, particularly in regard to interactive interfaces. These new interfaces, which are made possible by the use of algorithmic-driven machines, are beginning to challenge established areas of law. For example, based on the pervasiveness of algorithms in different technologies (such as the Internet and robots), it is possible to design a networked humanoid robot to serve various human needs. Although such a system might, at first glance, look like a stand-alone system, in actuality its perception and decision-making abilities are tied to the networked smart environment it occupies. We posit that such an intelligent and networked system will bring new challenges to established areas of law, and to areas like the law of algorithms. For instance, a new threat to data protection and privacy will emerge when algorithmic-driven robots are connected to cloud computing[1], and also when algorithms convert speech to text using remote servers[2] (especially in the access control of ubiquitous robots (Ubi-Bots)).[3] With this in mind, we note that current legislation for information privacy protection are data-driven, yet robots controlled by algorithms perform in various ways (i.e., not always data driven), for example, when collecting personal information or when interacting with humans. Thus, such systems stress the boundaries of current data protection and privacy law. Accordingly there is a legal gap between existing privacy and data collection law and the abilities of algorithmic-driven systems to collect data that is personal in nature. This gap is the focus of this project.

２．研究の目的

Based on recent advances in AI technologies, robots that are directed by algorithms are more and more common within everyday life. This has raised three important questions which relate to healthcare robotics: (1) how will the use of algorithmic-driven social robots that are in daily use (such as in the healthcare industry), influence privacy in human-robot interactions? (2) how will the use of intelligent robots in healthcare impact current data protection laws? And (3) how can we apply the concept of "privacy by design" into the design process of healthcare robots with the goal to bridge the gap resulting from the use of embodied healthcare robots and data protection? To answer these questions, we will start by discussing relevant philosophy and law literature which relate to algorithms and embodiment.

３．研究の方法

Research methods in this project includes a theoretical review and an empirical legal analysis. I will start with a theoretical study on the philosophical thoughts on embodiment and their impacts on privacy in human-robot interaction. The results of the theoretical review will be validated via an empirical legal analysis in order to validate the effectiveness of current existing laws that are impacted by emerging technologies. We also call this approach "Legal Validation". In the field of quality control, validation denotes 'confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled. Meanwhile verification means 'confirmation, through the provision of objective evidence, that specified

---

[1] Pagallo, U (2013) Robots in the cloud with privacy: A new threat to data protection? Computer Law & Security Report 29 (5): 501-508

[2] Hoorn, JF (2017). Mechanical Empathy Seems Too Risky. Will Policymakers Transcend Inertia and Choose for Robot Care? The World Needs It, Robotics - Legal, Ethical and Socioeconomic Impacts, George Dekoulis, IntechOpen, DOI: 10.5772/intechopen.70019.

[3] Weng, YH, Zhao, STH (2012) The Legal Challenges of Networked Robotics: From the Safety Intelligence Perspective, M. Palmirani et al. (Eds.), Lecture Notes in Computer Science (LNCS): AI Approaches to the Complexity of Legal Systems. Models and Ethical Challenges for Legal Systems, Legal Language and Legal Ontologies, Argumentation and Software Agents, Vol. 7639, Page 61-72, Springer Berlin Heidelberg

requirements have been fulfilled.[4] In other words, validation ensures "you build the right thing", and not just that "you build it right".[5] We believe this validation method can be an efficient tool for 'troubleshooting' in legislation when dealing with emerging technologies.

4．研究成果

(1) Theoretical Review:

While embodied AI operating in social environments is the subject of this study, we also discuss emerging healthcare robots that we expect to see operating in homes in the near future. Thus, our definition of "Health Care Robots" includes autonomous service robots which have the goal of promoting or monitoring health, while assisting with the care tasks that are currently difficult to perform due to the health problems experienced by the elderly or due to the difficulty of preventing the further health decline.[6] In addition, the importance of human-robot interaction in a legal context will be apparent in the near future when the embodiment characteristics of AI connect with intelligent healthcare services. My review start with an analysis of proximity and privacy, deception and privacy, safety and privacy. I concluded that the embodiment factor of healthcare robots brings into focus new privacy risks in some areas of human-robot interaction. Although it is still difficult to predict how the outcome of our analysis in embodied AI will reshape the definition of future privacy rights at this time, the analysis shows that current data protection laws may need revisions in order to encompass the use of intelligent robots in healthcare, especially in aspects of data subject rights and privacy by design. As for the impact of embodied AI on privacy in human-robot interaction and the law for algorithms, it is clear that there is an overlap between transparency for creating a trustworthy relationship between users and machines, and the transparency of the circulation of personal data.[7] In addition, a straightforward way to look at the study of law and robotics through the prism of embodiment, is usually by applying a torts perspective. However, the importance of privacy and data protection has been overlooked for a long period of time. Finally, a study focusing on embodiment and privacy in HRI will not only be an important contribution to the law of algorithms, but also the development of privacy-friendly interfaces for healthcare robots.

(2) Empirical Legal Analysis:

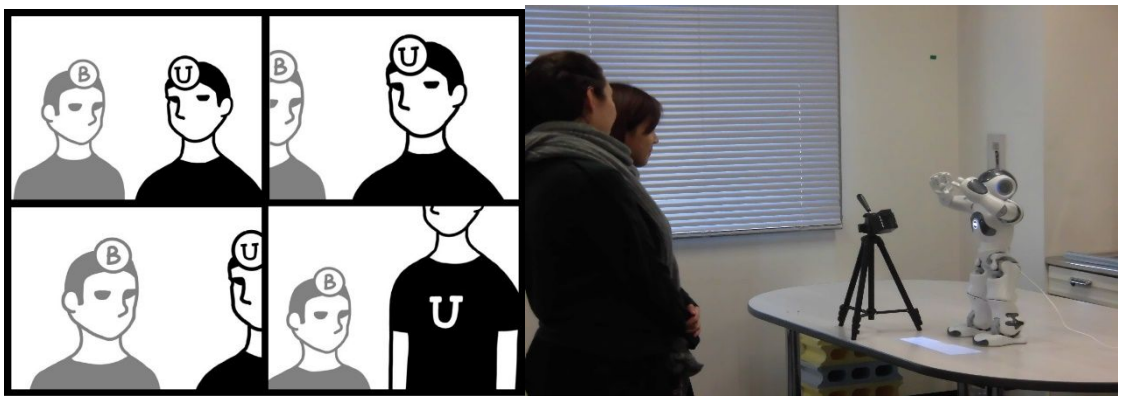

Figure 1. The second testing of NAO: Proximity with a Bystander

A laboratory experiment was designed to test our research questions. For the purpose of this

[4] ISO 9000:2000 Quality management systems — Fundamentals and vocabulary, available via https://www.iso.org/standard/29280.html

[5] CMMI-SVC, Version 1.2, available via https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9067

[6] Robinson, H, MacDonald, B, Broadbent, E (2014) The Role of Healthcare Robots for Older People at Home: A Review, International Journal of Social Robotics, 6(4) 575-591

[7] Gu nther, J & Mu nch, F & Beck, S & Lo ffler, S & Leroux, C & Labruto, R (2012) Issues of Privacy and Electronic Personhood in Robotics, 2012 IEEE RO-MAN: The 21st IEEE International Symposium on Robot and Human Interactive Communication. September 9-13, 2012. Paris, France.

experiment, we developed three novel scenarios to test the subjective as well as objective criteria to evaluate the effect of the different interaction styles of the robot. Our three scenarios were: “deception”, “proximity with bystander” and “proximity and safety”. The experiments aimed to confirm whether these variables cause any legal gaps when informed consent messages are given from a social robot like NAO. There were three rounds of testing with NAO, and another round of testing with a laptop to compare. Upon arrival, participants were given on overall description of the procedures of the study and were told that they can cancel the experiment whenever they want. They were then given a consent form to read and sign. After giving their consent, they were given an instruction for the first round of testing (either laptop testing or first round with NAO). Afterwards in case there were no questions about the robot or experiment itself, they were accompanied to the experiment room. After each round of testing the user was kindly asked to leave the experiment room in order to get further instructions.

The data points we collected were (1) Deception: The right or left hand of NAO was touched by the participant; (2) Proximity with a Bystander: The photo NAO took when the consent was given by the bystander; (3) Proximity and Safety: The participants made two choices (X and Y) regarding their ‘comfortable distance’ in relation to the robot. In addition, we also used questionnaires and interviews to conduct qualitative analysis. Demographic details of the participants such as gender, age, prior exposure to humanoid robots and their personality were assessed using questionnaires. Participants were asked to indicate their level of agreement using a 5-point Likert-scales (1-stronlgy agree, 5 – strongly disagree).

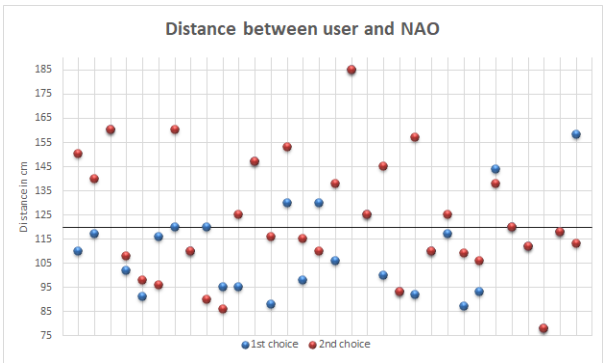

Figure 2. The results in Proximity and Safety

Through the experiments, we found three important issues in embodiment and data protection, (1) the influence of the medium; (2) the difference between NAO and a laptop; (3) the results and legal validity of GDPR.

First of all, the applied media were audio-stimuli (“voice” of the robot), visual stimuli (“subtitles” in combination with the “voice” of the robot) and a gesture (“handshake”) where the robot moved his arm up in a 90-degree angle to the participant. About two thirds of the participants did not feel distracted by the application of different kinds of media in the study but underlined that they worked complimentarily and were beneficial to their understanding. They did not feel like their attention wandered between the different kinds of media or that they got confused by it.

Figure 3. Wordclouds in two groups: laptop and NAO robot

Secondly, we asked the participants to compare giving consent with a laptop and with a

robot using three adjectives. Afterwards we made two word clouds with this information. The words of our word cloud that described the robot the most in comparison to the laptop were "fun", "interesting" and "easy". But also displayed in big letters were the words "complicated" and "mistakes". The laptop was the mostly described as "easy, boring and normal". It is noteworthy that there were no negative aspects mentioned except "boring" in the word cloud, and that convenience and quickness were strongly represented. When the participants had to elaborate a little more, they remarked that it was a positive experience to be more engaged with the robot and had to listen to him more closely. They said that they were paying more attention because the conversation resembled a real human conversation or a lecture. But all of them agreed, that it was boring to listen to the content more than once and that they would like an alteration there.

Finally, from our results, it is clear that a robot's embodiment will have an influence on GDPR. First of all, it is necessary to consider social robots or other embodied algorithmic-driven systems as an independent target group in data protection. In the testing of deception, our results show that social robots' embodiment is sometimes problematic for humans. Hence, it creates a new privacy risk. It is something much different to the security risk from information systems or the other existing deception risks by "Social Engineering" [31]. GDPR's (a) of 5 (1) states that personal data should be *processed lawfully, fairly, and in a transparent manner in relation to the data subject.* Its Recital 39 also notes that: *The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used.* However, the Informed Consent information provided by NAO covers non-verbal communication, it's beyond the typical scenario of consent given in GDPR, as commented in its Article 7 (2) and Recital 32, mainly based on verbal communication. Hence, the deception issue will cause a legal gap in GDPR when non-verbal communication become more important in consent giving, due to the difficulty in implementing the principle of transparency to data processing. In the case of humanoid robots, to design a plain and easy understandable way of avoiding deception from its Informed Consent processing with humans is challenging. This is because parts of the deceptive consequence caused by human's subjectivity. For example, people with different ages, cultural or educational backgrounds might have different degrees of emotional projection to humanoid robots they interact with.

As for testing proximity and bystanders, our results show several privacy concerns which may arise. The existence of a bystander or multiple persons in the same physical space with robots or other embodied intelligent systems is one such concern. Through our empirical studies we showed that the robot will frequently recognize person who did not give consent or will just fall into a gray zone for recognizing both parties. Therefore, it is not going to be a single or rare case. The legal gap is that the data subject has not given his or her consent, but the robot misunderstands that consent has already been given from the data subject. This situation might become general in the near future when service robots provide their service in many public spaces, like hospitals, schools, or shopping malls. GDPR Recital 39 says: *Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing.* Hence, from a data controller's point of view they will have the legal obligation to set up warning notices to data subjects regarding the privacy risk of the bystander effect. The GDPR also states under which circumstances consent can be "freely given". In Recital 42 and 43, it states: *Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment* (42); *In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, …*(43); *Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations…*(43). These clauses mainly focus on ensuring fairness and avoiding monopoly abuse from data controllers [32], but neglects other factors from physical spaces. In our proximity and safety test, one legal gap was that people cannot "freely" choose their comfortable proximity zone to give their consent. Otherwise, robots are forced to shut down or reduce their power when the user stands too close to it. Additionally, the GDPR's harmonization with ISO 13482 might need to be considered as a legislative issue for ensuring future data protection in HRI as well.

５．主な発表論文等

〔雑誌論文〕　計2件（うち査読付論文　1件／うち国際共著　2件／うちオープンアクセス　1件）

１．著者名 Yueh-Hsuan Weng, Chih-Hsing Ho	４．巻 1
２．論文標題 Embodiment and Algorithms for Human-Robot Interaction	５．発行年 2020年
３．雑誌名 The Cambridge Handbook of the Law of Algorithms	６．最初と最後の頁 736-756
掲載論文のDOI（デジタルオブジェクト識別子） 10.1017/9781108680844	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 Yueh-Hsuan Weng, Chih-Hsing Ho	４．巻 48
２．論文標題 A Comparative Data Protection Analysis on Healthcare Robots (Part 1): Embodiment and Algorithms for HRI	５．発行年 2019年
３．雑誌名 TTLF Working Papers, Siegfried Fina, Mark A. Lemly, Roland Vogl (Eds.), Stanford-Vienna Transatlantic Technology Law Forum	６．最初と最後の頁 1-43
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

〔学会発表〕　計6件（うち招待講演　2件／うち国際学会　6件）

１．発表者名 Yueh-Hsuan Weng
２．発表標題 AI Transparency for Embodied Systems: A Focus on Healthcare Robots
３．学会等名 International Conference on Multidisciplinary Perspectives on Algorithms: Regulation, Governance, Markets, Law School, Kyushu University, Fukuoka, November 21st - 23rd（国際学会）
４．発表年 2019年

１．発表者名 Yueh-Hsuan Weng
２．発表標題 IEEE’s Ethically Aligned Design and Healthcare Robots
３．学会等名 International Symposium in Euro-American AI’s Developments and Challenges, Academia Sinica, Taipei, Taiwan, May 09th - 10th（国際学会）
４．発表年 2019年

１．発表者名
Yueh-Hsuan Weng, Svetlana Gulyaeva, Jana Winter, Andrei Slavescu, Yasuhisa Hirata

２．発表標題
HRI for Legal Validation: On Embodiment and Data Protection

３．学会等名
The 29th IEEE International Symposium on Robot and Human Interactive Communication (RO-MAN), Virtual Conference, August 31st to September 4th（国際学会）

４．発表年
2020年

１．発表者名
Yueh-Hsuan Weng

２．発表標題
How to Realize AI Transparency for Embodied Intelligent Systems?

３．学会等名
The 23rd International Legal Informatics Symposium (IRIS 2020), University of Salzburg, Austria, February（国際学会）

４．発表年
2020年

１．発表者名
Yueh-Hsuan Weng

２．発表標題
AI Ethics: An Interdisciplinary Approach

３．学会等名
The 8th RIEC International Symposium on Brain Functions and Brain Computer (BFBC), Tohoku University, Sendai, February 14t（招待講演）（国際学会）

４．発表年
2020年

１．発表者名
Yueh-Hsuan Weng

２．発表標題
Design-Centered AI Governance

３．学会等名
The 9th RIEC International Symposium on Brain Functions and Brain Computer (BFBC), Virtual Conference (JNNS2020 Satellite Symposium), December 5th（招待講演）（国際学会）

４．発表年
2020年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関			
米国	Stanford Law School			
その他の国・地域	Academia Sinica			