The Lord of the (speaking) Rings: An interdisciplinary Fellowship to deal with 7 legal issues

Gianluigi M. Riva
University College Dublin
gianluigi.riva@ucd.ie

Marguerite Barry
University College Dublin
marguerite.barry@ucd.ie

ABSTRACT

One smart speaker to rule them all, one sensor to find them, one device to bring them all and in the Internet of Things bind them. Conversational User Interfaces (CUI) represent an interactive phenomenon that is disrupting social interactions as we knew them. The spectrum of legal issues that arises from these user-device relationships has a wide range of impacts on society. This paper addresses seven legal issues arising from these interactions that affect Privacy and Law concerning consumer protection, profiling, liability, security, neutrality, influence and data protection. It aims to prompt an interdisciplinary discussion between Human-Computer Interaction, legal and Privacy researchers in order to address the lack of regulation around aspects of CUI and stimulate legal, policy and design confrontations.

CCS CONCEPTS

• **Applied computing** → **Law**; • **Security and privacy** → **Human and societal aspects of security and privacy**; • **Human-centered computing** → *Natural language interfaces*; *Empirical studies in HCI*.

KEYWORDS

Conversational User Interfaces, Law, Privacy, HCI, IoT, AI, PbD

ACM Reference Format:

Gianluigi M. Riva and Marguerite Barry. 2020. The Lord of the (speaking) Rings: An interdisciplinary Fellowship to deal with 7 legal issues. In *2nd Conference on Conversational User Interfaces (CUI '20)*, July 22–24, 2020, Bilbao, Spain. ACM, New York, NY, USA, 3 pages. <https://doi.org/10.1145/3405755.3406132>

1 INTRODUCTION

Surveillance capitalism [18] is entering a new phase, in which interconnected ecosystems are gradually surrounding users. CUI systems will soon become our home butlers, office secretaries and portable friends [5]. Yielding (all) our personal data is the fee we pay for their useful services. This is an intrinsic “take it or leave it” condition [15] because without personal data, these systems cannot work [1]. However, at the same time service providers exploit the same data for purposes that do not reflect customers’ interests. Thus, the service has a double nature: one positive in plain

sight and another, dark and hidden. These devices represent another step toward 24/7 tracking enabled by the Internet of Things (IoT), entailing many privacy concerns regarding the abuse of profiling and data processing [3]. Here, we reflect on seven crucial yet under-researched legal issues pertinent to CUI systems, calling for prospective rather than retrospective legal approaches.

2 LEGAL ISSUES WITH SAURON’S EYE

2.1 Gollum is here to serve master Frodo

Would people be happy to be crash test dummies or drive cars tested directly on consumers? The Law would not allow it due to “precaution” principles. However, this already happens with CUIs, as terms and conditions (TCs) of many smart devices state that “X may collect, and your device may capture, voice commands and associated texts so that we can improve our technology providing you with better services and features”. Thus, profiling activities are not only used to shape content and features for specific users, or to sell tailored advertisements or products, but are also exploited for AI training purposes and consumer tests. For example, Facebook’s recent #10yearschallenge represented a simple way to train facial-recognition AI on ageing without user awareness [10, 16]. We do not allow direct tests of cars on customers as physical safety is an immediate perception. Yet, psychological and social repercussions are no less dangerous, they just reveal themselves in the longer term. While it is hard to define the correct metrics to set a threshold to benchmark these cases, we need precise regulation to address precise phenomena related to AI systems and their effects. Privacy regulation must be upgraded to face the challenges of cumulative impacts over time and standardisation may be the right path.

2.2 When the ring decides on your behalf

CUIs in IoT environments can be set up to perform automated decisions based on user settings or behaviours (i.e. profiling). For instance, we may set up an assistant to autonomously buy a product when out of stock (e.g. Amazon button), or to set our preferred room temperature using sensors that gather users’ habits. These useful services however, can create unexpected outcomes, due to misinterpretation, errors, and sensor misperceptions. Such wrongdoing that causes harm, damage, or mistaken relationships with third parties (such as ordering caviar instead of crackers), creates a whole set of legal implications. It involves both liability and black-box issues, as well as forcing users to prove a mistake, which, as well as being time-consuming and costly may be beyond their capacity. Private law urgently needs to address AI agency and its representative powers and effects in legal relationships [2].

This work is licensed under a Creative Commons Attribution International 4.0 License.

CUI '20, July 22–24, 2020, Bilbao, Spain

© 2020 Copyright held by the owner/author(s).

ACM ISBN 978-1-4503-7544-3/20/07.

<https://doi.org/10.1145/3405755.3406132>

2.3 Gandalf, what did you mean?

In 2018, a case occurred in the US where Alexa picked up a fight between a couple and sent the conversation via email to the husband's employee [16]. Language skills are a core element for effective CUI systems [4, 7]. Nevertheless, human language is full of shades, accents, inflections, assonances and even mistakes, such that people sometimes do not understand each other. However, comprehensibility is not a one-way issue: CUI must correctly understand users, and vice versa. Indeed, when interactions become more complex than merely a 'lights on' order, CUI could guide users with instructions to accomplish several activities. For the sake of liability, users must understand these instructions correctly. Who is liable for CUI mistakes? Consumer Law must protect users against being charged by service providers with this responsibility through terms and conditions.

2.4 My treasure. Only mine

Interfaces are now 'general', meaning everybody can interact with them. Soon they will become 'personal' and activated only by the owner or could have different profiles for different users. Nonetheless, a third party's CUI can be activated remotely [9] and it is further possible to activate an interface with non-audible frequencies [17]. Thus, there are serious security issues with a personal interface, as vocal recordings and images can be easily used to bypass voice and facial recognition passwords. This entails a security breach and the power to perform actions on behalf of users, who will not be in the position to prove that third parties caused those actions. Users should be empowered with full accessibility to data and metadata to be able to prove their estrangement to CUI misuse.

2.5 Théoden, can't you recognise friends?

Nowadays, we can usually recognise if we are talking to an autonomous agent or a human. However, since the advent of Google Duplex, which can mimic human linguistic features, such as tones, pauses and inflections [8], it is less evident. This represents the future of 'general' interface interactions in public smart-spaces or via smartphone. When we interact with each other, we are on an equal level of potential knowledge, comprehension, and information accessibility. However, when we interact with an AI agent that is able to gather information from Big Data, access profiling databases, and track users in real-time, we are in a weak, asymmetrical and unbalanced position. Recognisability should be a legal requirement for both AI (and CUI) and embodied agents (robots) in order to protect user privacy and awareness.

2.6 Samwise's loyalty to his master Frodo

A user-CUI relationship could develop a certain degree of affection, especially with long-term use, made even deeper with personalisation and interactive emotional feature design [6]. Addiction to or dependence on these systems is a related risk, especially for minors [13]. Aside from the social and psychological implications, the Law is concerned with the potential for influence on decision-making processes, affecting contractual relationships between users and CUI service suppliers. Indeed, service suppliers could have both a dominant position and conflict of interest if exploiting users' affection to influence their preferences, their commercial and political

opinions, behaviours and contractual choices [14]. Data Protection, Consumer, Competition and Private Law needs to be harmonised and upgraded to prevent this scenario. Making the use of a human voice in CUI systems illegal may seem a drastic solution but it would also address the recognisability issue described above.

2.7 When Frodo trusts Gollum blindly

CUIs will be soon the primary device for information access in an IoT environment [11]. They will assume the role played until now by search engines and smartphones. The filtering power they will manage around information, and related results will be enormous [14]. Search engines allow visual interaction with results and a choice among them, but in audio-vocal communications fewer results will be listed. Furthermore, we will not have any visual interaction with results. Therefore, the service suppliers' ability to shape outcomes and influence users' opinions will increase accordingly. This implies that CUIs will be the filters of every search, result, relationship and action with the IoT world, reflecting the potential monopoly of Sauron's eye [14]. The Law (and HCI design) must ensure CUI neutrality and regulating its filtering power for both ethical, contractual and privacy reasons. Regulation of content delivery through CUIs can ensure that transparency, accessibility and plurality principles remain intact in digital communication as well as the right to information.

3 CONCLUSIONS

Without proper regulation, the IoT could be the land of Mordor: ruled by the law of the strongest. CUI design impacts on important aspects of socio-legal systems that must be considered in advance by all stakeholders. There is a distinct opportunity for the CUI and legal communities to play an important role, working together to design useful systems that are respectful and protective of their users [12]. Mutual comprehension and deeper cooperation between legal and CUI scholarship can help provide CUI developers with practical preventive solutions, inspired by Privacy by Design principles. This fellowship will change the way in which future CUIs will work and in which users' liberties and rights will be ensured and protected, or not... it is up to us.

ACKNOWLEDGMENTS

This research was funded by the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 722561.

REFERENCES

- [1] Amazon. 2020. Amazon.com Help: Alexa Terms of Use. <https://www.amazon.com/gp/help/customer/display.html?nodeId=201809740>
- [2] Francisco Andrade, Paulo Novais, José Machado, and José Neves. 2007. Contracting agents: legal personality and representation. 15, 4 (2007), 357–373. <https://doi.org/10.1007/s10506-007-9046-0>
- [3] Chola Chhetri and Vivian Genaro Motti. 2019. Eliciting Privacy Concerns for Smart Home Devices from a User Centered Perspective. In *Information in Contemporary Society (2019) (Lecture Notes in Computer Science)*, Natalie Greene Taylor, Caitlin Christian-Lamb, Michelle H. Martin, and Bonnie Nardi (Eds.). Springer International Publishing, 91–101. https://doi.org/10.1007/978-3-030-15742-5_8
- [4] Leigh Clark, Nadia Pantidi, Orla Cooney, Philip Doyle, Diego Garaialde, Justin Edwards, Brendan Spillane, Emer Gilmartin, Christine Murad, Cosmin Munteanu, Vincent Wade, and Benjamin R. Cowan. 2019. What Makes a Good Conversation? Challenges in Designing Truly Conversational Agents. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (2019-05-02) (CHI '19)*.

- Association for Computing Machinery, 1–12. <https://doi.org/10.1145/3290605.3300705>
- [5] Phil Cohen, Adam Cheyer, Eric Horvitz, Rana El Kaliouby, and Steve Whittaker. 2016. On the Future of Personal Assistants. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (2016-05-07) (*CHI EA '16*). Association for Computing Machinery, 1032–1037. <https://doi.org/10.1145/2851581.2886425>
  - [6] Sylvie Delacroix and Michael Veale. 2019. Smart Technologies and Our Sense of Self: Going Beyond Epistemic Counter-Profiling. <https://papers.ssrn.com/abstract=3372128>
  - [7] Robert A. Kennewick and Lynn Elise Armstrong. 2015. System and method for hybrid processing in a natural language voice services environment. <https://patents.google.com/patent/US9171541B2/en?q=Natural+language+processing+device&oq=Natural+language+processing+device>
  - [8] Yaniv Leviathan and Yossi Matias. [n. d.]. Google Duplex: An AI System for Accomplishing Real-World Tasks Over the Phone. <http://ai.googleblog.com/2018/05/duplex-ai-system-for-natural-conversation.html>
  - [9] Sapna Maheshwari. 2017. Burger King 'O.K. Google' Ad Doesn't Seem O.K. With Google. (2017). <https://www.nytimes.com/2017/04/12/business/burger-king-tv-ad-google-home.html>
  - [10] Nicole Martin. 2019. Was The Facebook '10 Year Challenge' A Way To Mine Data For Facial Recognition AI? <https://bit.ly/2B7g5QH>
  - [11] Kenichiro Noda. 2017. Google Home: smart speaker as environmental control unit. 13, 7 (2017), 674–675. <https://doi.org/10.1080/17483107.2017.1369589> Publisher: Taylor & Francis _eprint: <https://doi.org/10.1080/17483107.2017.1369589>.
  - [12] Hyuna Park and Eric Benson. 2013. Systems thinking and connecting the silos of design education. In *Proceedings of the 15th International Conference on Engineering and Product Design Education: Design Education - Growing Our Future, EPDE 2013* (2013-12-01). 277–281. <https://experts.illinois.edu/en/publications/systems-thinking-and-connecting-the-silos-of-design-education>
  - [13] Gianluigi M. Riva. 2020. Fantastic Interfaces and where to regulate them: Three provocative privacy reflections on truth, deception, and what lies between. In *Digital Transformation of Collaboration* (springer ed.). Springer Nature, Vol. Chapter 15. P. A. Gloor, A. Przegalinska, F. Gripp.
  - [14] Gianluigi M. Riva and Marguerite Barry. 2019. Net Neutrality matters: Privacy antibodies for information monopolies and mass profiling | Neutralidade da rede importa: anticorpos de privacidade para monopólios de informação e profiling em massa. 5, 2 (2019), 7–35. <https://doi.org/10.12957/publicum.2019.47199>
  - [15] European Data Protection Supervisor. 2018. EDPS Opinion No. 3/2018 on online manipulation and personal data. , 31 pages. https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf
  - [16] Sam Wolfson. 2018. Amazon's Alexa recorded private conversation and sent it to random contact. (2018). <https://www.theguardian.com/technology/2018/may/24/amazon-alexa-recorded-conversation>
  - [17] Guoming Zhang, Chen Yan, Xiaoyu Ji, Tianchen Zhang, Taimin Zhang, and Wenyuan Xu. 2017. DolphinAttack: Inaudible Voice Commands. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (2017-10-30) (*CCS '17*). Association for Computing Machinery, 103–117. <https://doi.org/10.1145/3133956.3134052>
  - [18] Shoshana Zuboff. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Ny Public Affirs.