good brother

INTERNATIONAL CONFERENCE ON PRIVACY-FRIENDLY AND TRUSTWORTHY TECHNOLOGY FOR SOCIETY

28 June 2022

Zagreb, Croatia

cost
European Cooperation in Science and Technology

HRZZ
Croatian Science Foundation

Digit-HeaL

Proceedings of the 2022 GoodBrother International Conference on Privacy-friendly and Trustworthy Technology for Society

Authors[1]

Anto Čartolovni, Catholic University of Croatia, Croatia
Anton Fedosov, University of Zurich, Switzerland
Eduard Fosch-Villaronga, Leiden University, the Netherlands
Christoph Lutz, BI Norwegian Business School, Norway
Aurelia Tamò-Larrieux, Maastricht University, The Netherlands

Keywords

Privacy, Trust, Trustworthiness, Society, Active and Assisted Living, AAL Technologies

Preface

The GoodBrother COST Action (CA19121) on *Privacy-Aware Audio- and Video-Based Applications for Active and Assisted Living*[2] organized a hybrid conference on *'Privacy-friendly and trustworthy technology for society'* that took place on 28 June 2022 in Zagreb, Croatia, and online on Zoom as well as YouTube. With this conference, we aimed to advance the knowledge on critical ethical concepts such as privacy, trust, and transparency of (AAL) technologies, contributing particularly by extending emerging themes such as privacy-by-design, overtrust, transparency-by-design, and personalized transparency. Throughout the conference, the participants explored links, overlaps, and solutions between current proposed regulations such as the AI Act and other enforced regulations like the General Data Protection Regulation and the Medical Device Regulation. The organizers invited interdisciplinary approaches spanning the social sciences, legal scholarship, ethics, and research in computing and engineering.

We received a large number of submissions in Spring 2022 from the authors in Australia, the US, Singapore, the UK, the EU, Norway, and Switzerland, accepting 16 papers based on the score and the feedback from two reviewers with expertise in computer science, ethics, law, and communication science. The papers were selected based on their quality and the fit with the conference theme. The reviews were sent with the acceptance/rejection email, and the camera-ready versions had to incorporate the reviewers'

[1] In alphabetical order
[2] *See* https://goodbrother.eu/

feedback. We subsequently invited the authors of the accepted submissions to extend their ideas during their presentations organized in three thematic sessions[3].

Audience and format

We welcomed and encouraged interdisciplinary research and collaborations among researchers active in different working groups. The presentations were approximately 15 min long, followed by a brief Q&A. The focus rested on the discussions among participants and establishing potential links among ongoing research activities within the COST Action and beyond. The conference was kick-started by an opening keynote of Prof. Dr. Esther Keymolen on the topic of trust and trustworthiness, and closed by a keynote of Associate Prof. Dr. Jaap-Henk Hoepmann presenting his newest research on privacy by design.

Submissions and expected outcomes

The abstracts here compiled in the proceedings will be complemented by a special issue[4] in *Digital Society* (Springer) that convenes full paper submissions on the conference theme and is targeted at conference presenters and beyond.

Cost Action GoodBrother

This conference was supported by the COST Action CA19121 Network on Privacy-Aware Audio- and Video-Based Applications for Active and Assisted Living, also named *GoodBrother*. GoodBrother aims to increase the awareness of the ethical, legal, and privacy issues associated with audio- and video-based monitoring and to propose privacy-aware working solutions for assisted living by creating an interdisciplinary community of researchers and industrial partners from different fields (computing, engineering, healthcare, law, sociology) and other stakeholders (users, policymakers, public services), stimulating new research and innovation. GoodBrother will offset the "Big Brother" sense of continuous monitoring by increasing user acceptance, exploiting these new solutions, and improving market reach.

Suggested Citation for the conference proceedings volume

Anto Čartolovni, Anton Fedosov, Eduard Fosch-Villaronga, Christoph Lutz, and Aurelia Tamò-Larrieux (2022): Proceedings of the 2022 GoodBrother International Conference on Privacy-friendly and Trustworthy Technology for Society – COST Action 19121 - Network on Privacy-Aware Audio- and Video-Based Applications for Active and Assisted Living. Zagreb, Croatia, June 28, 2022.
DOI:10.5281/zenodo.6813377

[3] *See* the conference program here https://goodbrother.eu/conferences/goodbrother-international-conference-on-privacy-friendly-and-trustworthy-technology-for-society/ with sessions on Technology Meets (Privacy) Law, Ethics, and Society; Privacy and Trust Perceptions; and Social Issues and Contextual Questions

[4] *See* the special issue call for paper here: https://link.springer.com/collections/ccfheehheh

Acknowledgements

This publication is based upon work from COST Action CA19121, supported by COST (European Cooperation in Science and Technology).

COST (European Cooperation in Science and Technology) is a funding agency for research and innovation networks. Our Actions help connect research initiatives across Europe and enable scientists to grow their ideas by sharing them with their peers. This boosts their research, career and innovation.

www.cost.eu

https://goodbrother.eu

http://cost.eu/actions/CA19121/

Table of Contents

Liane Colonna (2021): Addressing the Responsibility Gap in Data Protection by Design: Towards a More Future-oriented, Relational, and Distributed Approach. In: Proceedings of the International Conference on Privacy-friendly and Trustworthy Technology for Society – COST Action CA19121 - Network on Privacy-Aware Audio- and Video-Based Applications for Active and Assisted Living

Addressing the Responsibility Gap in Data Protection by Design: Towards a More Future-oriented, Relational, and Distributed Approach

Liane Colonna
Department of Law, Stockholm University, Sweden
Liane.Colonna@juridicum.su.se

Zaira Zihlmann, Kimberly Garcia, Simon Mayer, and Aurelia Tamò-Larrieux (2022): A right to repair privacy-invasive services: Is a new, more holistic European approach emerging? In: Proceedings of the International Conference on Privacy-friendly and Trustworthy Technology for Society – COST Action CA19121 - Network on Privacy-Aware Audio- and Video-Based Applications for Active and Assisted Living

A right to repair privacy-invasive services: Is a new, more holistic European approach emerging?

Zaira Zihlmann[1], Kimberly Garcia[2], Simon Mayer[2], and Aurelia Tamò-Larrieux[3]
[1] University of Lucerne, Lucerne, Switzerland
[2] University of St. Gallen, St. Gallen, Switzerland
[3] Maastricht University, Maastricht, The Netherlands
zaira.zihlmann@unilu.ch; kimberly.garcia@unisg.ch; simon.mayer@unisg.ch; a.tamo@maastrichtuniversity.nl

Abstract

The terms of use of online services are often constructed as binary options which leads to take-it-or-leave-it decisions by users: either one agrees to the data processing practices of the service provider and gets access to the service, or one does not agree and cannot use the service. Research shows that consent notices do not provide actual control to users over how their data is being processed due to numerous reasons, such as not reading policies (Custers et al., 2018), privacy fatigue (Choi, Park and Jung, 2018), and manipulative designs (Waldman, 2020). Against this backdrop we conceptualized a right to customization that should provide users with the right to demand that virtual services are customized in a manner that reflects their privacy needs (Tamò-Larrieux et al., 2021). Our concept

roots in the GDPR, specifically on the right to data portability (Article 20) and on the principle of data protection by design and default (DPbDD) enshrined in Article 25. We argue that DPbDD enables data subjects to demand technical and organizational measures to be put in place and that operalizing DPbDD requires thinking about the whole life cycle of data, individual rights, the ideas of individual participation and control aspects. Furthermore, we use the right to repair as a source of inspiration. Calls to update the right to repair to include obsolete software have been raised and recently the CJEU *de facto* recognized a right to repair for software in the case Top System SA v Belgian State[1] (van Holst, 2021). This fundamentally changes the scope of repair and should according to our analysis be broadened even more to include modifications of software-based services for better privacy protection.

From a technical perspective the key question becomes how to empower individuals with respect to their data. The right to customization could be achieved through two technological approaches, namely service variants and service alternatives. In the former, a Data Controller (DC) creates and actively curates a catalog of software variants that collect and use different types of user data to provide the same (or very similar) functionality. Thus, users can opt for highly personalized experiences or just the service core functionality. In the latter approach, the DC provides interoperable and interchangeable service alternatives allowing users to retain control of their data by granting fine-grained access to it (e.g., through Solid, the Social Linked Data project[2]). In practice, this would mean that e.g., users of a voice assistant could, based on the right to customization, require the DC to apply certain restrictions to the service, such as restricting the recording of voices at a certain time of day or removing recordings of children's voices before cloud uploads. In this scenario, the DC would either have to create a variant that implements the users' customization requests or allow the use of another service that makes these customizations before uploading the data.

We see further technical developments heading in the same direction as we do with our proposal towards considering service variants and alternatives. For instance, the Smart Speaker Blocker (Olade et al., 2020) is an intermediary device that aims to intelligently filter out sensitive conversations and thus prevents this information from reaching a microphone in the first place. Users should even have the possibility to completely hide all identifying information by allowing the smart speaker only to receive a synthesized text-to-speech voice. Instead, Cheng et al. (2019) aim to provide users with control over the recording behavior of voice assistants. They propose that a user could employ a tagging device that emits an acoustic signal and signals the system that the user does at the moment not consent to recording. Another technology development that shows the feasibility of creating

[1] CJEU judgment of 6 October 2021, Top System SA v Belgian State, case C-13/20, EU:C:2021:811.

[2] https://solidproject.org/

service variants is Apple's App Clips for iOS[3]. App Clips are a small part of an app that provide a specific functionality. Thus, users do not need to install software that they might never use, or sign up for accounts that might be only used once. Tracking data is limited in App Clips and they are automatically removed from a device 30 days after they are used.

With respect to service alternatives, we see first implementations for instance by the Flemish government that is currently testing Solid for public services via the "My Citizen" profile. The profile brings together data from different parts of the administration into a single, easily accessible application. Through their profile, citizens can then access a personal overview of government services and can navigate to the respective service. This furthermore allows citizens to share personal information with government entities while their data remains within the personal data store (CDEI, 2021).

While the technical tools described above and the Flemish project show that it is technically and politically feasible to give more control to users, there are also some limitations: From the user's perspective, exercising the right to customization requires a deeper understanding of the system which can have a negative impact on the ease of use. To tackle this issue, we envision "customization communities", analogous to the emergence of so-called Repair Cafés that facilitate exercising the right to repair. Furthermore, the role of intermediary services such as Solid, needs to be further analyzed and qualified in order to identify the potential risks and challenges they encounter (e.g., their responsibility in case there is a data breach in the Pod). This aspect is related to the absence of a legal framework that comprehensively underpins and guides these technological efforts.

However, developments in this direction are emerging in the EU as we see new regulations that push towards the empowerment of individuals with respect to their data. In its communication "A European strategy for data", the EU Commission states that "[i]ndividuals should be further supported in enforcing their rights with regard to the use of the data they generate. They can be empowered to be in control of their data through tools and means to *decide at a granular level* about what is done with their data ('personal data spaces')" (European Commission, 2020, p. 20, emphasis added). According to the Commission, this could be achieved by strengthening the right to data portability, e.g., by imposing stricter requirements on interfaces for real-time data access and the mandatory use of machine-readable formats for data from certain products and services, such as data from smart home devices. Beyond that, rules for new types of data intermediaries such as providers of 'personal data spaces' might be considered. The Commission is aware of technical tools such as Solid that enable users to decide at a granular level what happens to their data, and it recognizes the great potential of these tools as well as the need for a supportive environment for them (European Commission, 2020).

---

[3] https://developer.apple.com/app-clips/

Legislative action in this respect is underway. First, we can observe that the proposal for a Regulation on Privacy and Electronic Communications[4] points to the initially described issues of consent and states that users should have the possibility to grant consent through software settings and providers of software are encouraged to include settings in their software which allows end-users to manage consent (Recital 20a). Heading in the same direction, the recently proposed Data Act[5] aims to empower individuals with respect to their data as well as to enhance innovation and competition among EU businesses. It inter alia foresees provisions that should permit users of connected devices to access the data they generate and to share it with third parties so that these can offer aftermarket or other data-driven services (European Commission, 2022). Another legislative initiative from the European strategy for data is the Data Governance Act (DGA)[6]. Amongst others, the DGA introduces so-called "data intermediation services". Their main purpose is data sharing through technical, legal, or other means (Article 2(2a)). According to Recital 23 such services would "enhance individual agency and in particular the individuals' control over the data relating to them" and notably help to exercise data subjects' rights under the GDPR. It is envisaged that this could be done by using personal information management tools like personal data spaces or data wallets (Slovenian Presidency of the Council of the European Union, 2021). Looking at the DGA's provisions on data intermediation services, one may conclude that Solid may be such an intermediary (CDEI, 2021).

Yet, the idea of data intermediation services is not the only trace leading in the direction of what we call the right to customization. We think that looking at current legal developments in the EU one can observe a move towards a more holistic approach that allows data subjects to exercise personalized control over their data. We believe that with our concept of a right to customization we might be able to capture the current legal, political, and technical developments, thereby making them available for a nuanced and goal-oriented discourse.

---

4 Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Mandate for negotiations with the European Parliament, Brussels, 10.2.2021.

5 European Commission, Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), Brussels, 23.2.2022, COM(2022) 68 final 2022/0047.

6 Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act) - Mandate for negotiations with the European Parliament, Brussels, 24.9.2021.

References

European Commission (2020): ‘Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European strategy for data’, Brussels, 19.2.2020, COM(2020) 66 final.

European Commission (2022, February 23): ‘Data Act: Commission proposes measures for a fair and innovative data economy’, press release, Brussels, retrieved April 7, 2022 from https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_22_1113/IP_22_1113_EN.pdf.

Centre for Data Ethics and Innovation (CDEI) (2021, July 22): ‘Unlocking the value of data: Exploring the role of data intermediaries’, retrieved April 7, 2022 from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1004925/Data_intermediaries_-_accessible_version.pdf.

Cheng, P. et al. (2019): ‘Smart Speaker privacy control - acoustic tagging for Personal Voice Assistants’, *IEEE Workshop on the Internet of Safe Things*, 23 May 2019, San Francisco, California, United States.

Choi, H., Park, J. and Jung, Y. (2018): ‘The role of privacy fatigue in online privacy behavior’, *Comput. Hum. Behav.* 81, pp. 42–51.

Custers, B. et al. (2018): ‘Consent and privacy’, in: A. Müller and P. Schaber (eds.): *The Routledge Handbook of the Ethics of Consent*, Routledge, London, 2018, pp. 247–258.

Olade, I. et al. (2020): ‘The Smart2 Speaker Blocker: An Open-Source Privacy Filter for Connected Home Speakers’, *arXiv*, arXiv:1901.04879v3.

Slovenian Presidency of the Council of the European Union (2021, October 1): ‘EU looks to make data sharing easier: Council agrees position on Data Governance Act’, press release, retrieved April 7, 2022 from https://slovenian-presidency.consilium.europa.eu/en/news/eu-looks-to-make-data-sharing-easier-council-agrees-position-on-data-governance-act/

Tamò-Larrieux, A. et al. (2021): ‘The Right to Customization: Conceptualizing the Right to Repair for Informational Privacy’, in: N. Gruschka et al. (eds.): *Privacy Technologies and Policy*, APF 2021, Lecture Notes in Computer Science, vol 12703, Springer, Cham, 2021, pp. 3–22.

van Holst, W. (2021, October 20): ‘Top system and the right to repair’, retrieved April 7, 2022 from https://edri.org/our-work/top-system-and-the-right-to-repair/.

Waldman, A.E. (2020): ‘Cognitive biases, dark patterns, and the ‘privacy paradox.’’, *Curr. Opin. Psychol. 31*, pp. 105–109.

Zhicheng He (2022): Bridging Law and Technology: Seeing Through Privacy-Enhancing Technologies for Assisted Living from the Perspective of EU Data Protection Law. In: Proceedings of the International Conference on Privacy-friendly and Trustworthy Technology for Society – COST Action CA19121 - Network on Privacy-Aware Audio- and Video-Based Applications for Active and Assisted Living

Bridging Law and Technology: Seeing Through Privacy-Enhancing Technologies for Assisted Living from the Perspective of EU Data Protection Law

Zhicheng, He
The Swedish Law and Informatics Research Institute, Faculty of Law, Stockholm University
zhicheng.he@juridicum.su.se

Naomi Lintvedt (2022): Thermal Imaging in Robotics as a Privacy Enhancing or Privacy Invasive Measure? The Necessity of a Holistic Approach to Privacy in Human-Robot Interaction. In: Proceedings of the International Conference on Privacy-friendly and Trustworthy Technology for Society – COST Action CA19121 - Network on Privacy-Aware Audio- and Video-Based Applications for Active and Assisted Living

Thermal Imaging in Robotics as a Privacy Enhancing or Privacy Invasive Measure? The Necessity of a Holistic Approach to Privacy in Human-Robot Interaction

Naomi Lintvedt
Norwegian Research Center for Computers and Law, University of Oslo, Norway
m.n.lintvedt@jus.uio.no

The conflicting use of thermal imaging in robotics

When robots interact with humans, how to preserve the privacy of the human users is a concern, including what the robot 'sees.' In some robotics research, the use of thermal imaging is chosen to 'conceal the individual's identity' (Valdivelu et al., 2017). The emphasis is on masking identifiable information in the images, such as details of the face, by using thermal cameras instead of regular RGB cameras (Schulz et al., 2018). The assumption is that once the clear facial image of a person is removed, the person is no longer identifiable, thus privacy is protected. Thermal imaging is for example proposed to be used in fall detection in bathrooms for elderly people and patients. Instead of a robot or a person following the person into the bathroom, the robot mounted with a thermal imaging camera can be outside the room, thereby presumedly preserving the privacy of the person not being observed during activities in the bathroom (Kido et al., 2009).

By contrast, other robotics researchers explore the possibility of using thermal imaging to improve or personalize human-robot interaction. Thermal cameras are for example used in robots to monitor physiological changes in elderly persons by detecting subtle changes in facial temperatures (Coşar et al., 2018); emotion recognition in children tracking facial landmarks during child-robot interaction (Goulart et al., 2019); and to detect emotions with the aim of strengthening the human-robot interaction (Pavladis et al., 2002). Other possible use areas for thermal imaging are to detect deceit by recording the thermal patterns from faces, i.e., as a polygraph (Pavladis et al., 2002); gender recognition (Nguyen et al., 2017); pain monitoring (Erel & Özkan, 2017); detection of sexual arousal (Liberati & Nagataki, 2019); monitoring of diseases (Brzezinski et al., 2021); or for fever detection or monitoring (Yang et al., 2020).

Hence, thermal imaging can reveal personal information which is hidden from view, such as health data and emotions. Another intrusive property of the technology is that it can detect people through barriers, unlike a regular camera. Thermal imaging is therefore magnifying the capacity to observe and enhances the robot's ability to detect and process personal data.

The misconception of privacy

In robotics research, privacy is most often understood as informational privacy or not defined at all (Lutz et al., 2019). Similarly, when robotics research on the use of thermal imaging refers to preserving or protecting privacy, privacy is understood as a person not being seen clearly. By obscuring or removing the facial image, or not seeing the body of the person, privacy is maintained. However, this simplified view of privacy fails to recognise that informational privacy is only on type of privacy (GoodBrother, 2021), in addition to bodily, spatial, communicational, proprietary, intellectual, decisional, associational, and behavioural privacy (Koops et al., 2017). These notions of privacy are particularly relevant for robots due to both their physical presence and complex data processing capacities (Fosch-Villaronga, 2019). Although legal researchers have addressed privacy in robotics, this seem to be lost in translation when crossing-over to other fields of robotics research, which leaves a gap between the technical and legal research. As Rueben et al. (2018) has proposed, privacy-sensitive robotics should be concerned with all different aspects of privacy.

Thermal cameras as privacy preserving tools are based on the notion that the robot will then not 'see'. But does the robot 'see'? The robot itself will not be interested in the images of people. Whether it needs images or not to function, is dependent on its purpose. This also extends to the use of thermal imaging. If the robot needs to 'see' to be able to not only detect, but to identify a person, it will need the data feed from the RGB cameras, e.g., the robot needs to ascertain that it is administering medicine to the right person. A robot may also need to use several

sensors, including thermal imaging, to be able to detect, identify and interact properly and safely with that person. Using anthropomorphic language to describe the robot's features thus obscures the actual features and complexities of the technology (Grimm, 2021).

The anthropomorphic design of robots raises concerns that the design may give users a false sense of comfort (Rueben & Smart, 2016). A robot closing its 'eyes' or turning its back to the user may make the user more comfortable and at first glance may seem privacy friendly (Yang et al., 2022). However, thermal cameras and other sensors may be placed elsewhere on the robot and not designed as eyes (Kaminski et al., 2017). Thus, these techniques may reassure the user, while at the same time be deceiving as to the full scope of what the robot is 'sensing'. Kamenski et al. (2017) have suggested a principle of 'honest anthropomorphism' to avoid deliberately misleading users as to what the robot is doing. On the same note Schafer & Edwards (2017), propose that robots should be built with their sensory capacity openly displayed. How, and if, this would be manifested in robotics design is another matter.

The use of thermal imaging as a replacement to RGB cameras is often based on an understanding that this will not be personal data (Hassan & Bessam, 2019; Tørresen, 2021), thus not acknowledging the intrusive nature of thermal imaging and the consequences for privacy. The different definitions of personal data across jurisdictions as well as the complexity and variety of the scope of privacy, may contribute to this confusion. As argued by Purtova (2018), the distinction between personal and non-personal data may no longer be meaningful with the increase of datafication and advances in data analytics and smart environments. This is particularly relevant for human-robot interaction where most, if not all, of the data can be related to an identifiable individual, whether the data is observations of the person or more technical data of the robot's performance. Applying a broad concept of personal data in robotics would ensure that data is treated as personal data, and reduce the risk of misconceptions such as treating data inferred from thermal imaging as non-personal data. Although this is an EU centric approach to personal data, the global nature of development of robotics would benefit from the most extensive definition being used instead of the lowest common denominator.

It is encouraging that privacy by design and data minimisation are addressed in robotics, but as the example of thermal imaging shows, replacing one sensor for another may not be privacy preserving but instead increases the invasiveness of the technology. Scherer's (2016) observations that the interaction between a variety of software and hardware components developed separately in various geographical locations increases the complexity of managing risks in AI, is even more pertinent for robotics. Instead of assessing each sensor in isolation, robot design must be considered in relation to its purpose and functionality. Hence, we need to ascertain a holistic approach to privacy in human-robot interaction. This will require cross-disciplinary work, where one of the contributions of legal scholars would be to

draw on the extensive privacy scholarship, as proposed by Rueben et al. (2018), and to clarify the notion of personal data in robotics, and how data can be minimised without compromising safety and security or even by increasing privacy risks.

Acknowledgments

Work on this abstract was carried out under the aegis of the research project 'Vulnerabilty in the Robot Society' ('VIROS'), funded by the Norwegian Research Council. Thanks are due to my colleagues in the VIROS project, and to the reviewers for encouraging and valuable comments.

References

Brzezinski, R. Y., Rabin, N., Lewis, N., et al. (2021): 'Automated processing of thermal imaging to detect COVID-19', *Scientific Reports*, vol. 11, no. 17489, September 2021, doi.org/10.1038/s41598-021-96900-9

Burkhard Schafer and Lilian Edwards (2017): '"I spy, with my little sensor": fair data handling practices for robots between privacy, copyright and security', *Connection Science,* 29:3, 200-209, DOI: 10.1080/09540091.2017.1318356

Coşar, S., Yan, Z., Zhao, F., Lambrou, T., Yue, S. and Bellotto, N. (2018): 'Thermal Camera Based Physiological Monitoring with an Assistive Robot', *40th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, July 2018, pp. 5010-5013, doi: 10.1109/EMBC.2018.8513201

Erel, V. K. and Özkan, H. S. (2017): 'Thermal camera as a pain monitor', *Journal of Pain Research*, vol. 10, November 2017, pp. 2827-2832, doi.org/10.2147/JPR.S151370

Fosch-Villaronga, E. (2019): *Robots, Healthcare, and the Law. Regulating Automation in Personal Care*, Routledge, London, doi.org/10.4324/9780429021930

GoodBrother (2021): 'State of the art on ethical, legal, and social issues linked to audio- and video-based AAL solutions', December 2021, https://goodbrother.eu/wp-content/uploads/2022/03/GoodBrother-State-of-the-art-on-ethical-legal-and-social-issues-linked-to-audio-and-video-based-AAL-solutions.pdf

Goulart, C., Valadão, C., Delisle-Rodriguez, D., et al (2019): 'Visual and Thermal Image Processing for Facial Specific Landmark Detection to Infer Emotions in a Child-Robot Interaction', *Sensors*, vol. 19, issue 13, June 2019, p. 2884, doi.org/10.3390/s19132844

Grimm, C. M. (2021): 'The danger of anthropomorphic language in robotic AI systems', *Brookings TechStream*, 18 June 2021, https://www.brookings.edu/techstream/the-danger-of-anthropomorphic-language-in-robotic-ai-systems/

Hassan, M. A. and Bessam A. (2021): 'Monitoring Indoor Activity of Daily Living Using Thermal Imaging: A Case Study', *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 9, September 2021, pp. 11-16, https://thesai.org/Downloads/IJACSA_Volume12No9.pdf

Kaminski, M. E., Rueben, M., Smart, W. D. and Grimm, C. M. (2017): Averting Robot Eyes, *Maryland Law Review*, vol. 76, issue 4, 2017, pp. 983-1024, https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=3761&context=mlr

Kido, S., Miyasaka, T., Tanaka, T., Shimizu, T. and Saga, T. (2009): 'Fall detection in toilet rooms using thermal imaging sensors', *2009 IEEE/SICE International Symposium on System Integration (SII)*, January 2009, pp. 83-88, doi: 10.1109/SI.2009.5384550

Koops, B-J., Newell, B. C., Timan, T., Škorvánek, I., Chokrevski, T. and Galič, M. (2017): 'A typology of privacy', *University of Pennsylvania Journal of International Law*, vol. 38, issue 2, 2017, pp. 483-57, https://scholarship.law.upenn.edu/jil/vol38/iss2/4

Liberati, N. and Nagataki, S. (2019): 'Vulnerability under the gaze of robots: Relations among humans and robots', *AI & Society*, vol. 34, May 2018, pp. 333-342, doi.org/10.1007/s00146-018-0849-1

Lutz, C., Schöttler, M. and Hoffmann, C. P. (2019): 'The Privacy Implications of Social Robots: Scoping Review and Expert Interviews', *Mobile Media & Communication*, vol. 7, issue 3, September 2019, pp. 412-434, doi.org/10.1177/2050157919843961

Nguyen, D. T., Kim, K. W., Hong, H. G., Koo, J. H., Kim, M. C. and Park, K. R. (2017): 'Gender Recognition from Human-Body Images Using Visible-Light and Thermal Camera Videos Based on a Convolutional Neural Network for Image Feature Extraction', *Sensors*, vol. 7, issue 3, March 2017, p. 637, doi.org/10.3390/s17030637

Pavlidis, I., Eberhardt, N. and Levine, J. (2002): 'Seeing through the face of deception', *Nature*, vol. 415, no. 35, January 2002, https://doi.org/10.1038/415035a

Purtova, P. (2018): 'The law of everything. Broad concept of personal data and future of EU data protection law,' *Law, Innovation and Technology*, vol. 10, no. 1, February 2018, pp. 40-81, doi: 10.1080/17579961.2018.1452176

Rueben, M. and Smart, W. D. (2016): 'Privacy in Human-Robot Interaction: Survey and Future Work', *WeRobot 2016,* https://robots.law.miami.edu/2016/wp-content/uploads/2015/07/Rueben_Smart_PrivacyInHRI_WeRobot2016.pdf

Rueben, M., Aroyo, A. M., Lutz, C. et al. (2018): 'Themes and Research Directions in Privacy-Sensitive Robotics,' *2018 IEEE Workshop on Advanced Robotics and its Social Impacts (ARSO)*, January 2019, pp. 77-84, doi: 10.1109/ARSO.2018.8625758

Scherer, M. U. (2016): 'Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies', *Harvard Journal of Law & Technology*, vol. 29, no. 2, May 2015, pp. 354-398, dx.doi.org/10.2139/ssrn.2609777

Schulz T., Herstad J. and Holone H. (2018): Privacy at Home: An Inquiry into Sensors and Robots for the Stay at Home Elderly', in J. Zhou and G. Salvendy (eds): *Human Aspects of IT for the Aged Population. Applications in Health, Assistance, and Entertainment. ITAP 2018. Lecture Notes in Computer Science*, vol. 10927, Springer, Cham., doi.org/10.1007/978-3-319-92037-5_28

Tørresen, J. (2021): 'Undertaking Research with Humans within Artificial Intelligence and Robotics: Multimodal Elderly Care Systems', *Technology Architecture + Design (TAD)*, vol. 5, no. 2, November 2021, pp. 141–145. doi: 10.1080/24751448.2021.1967052

Vadivelu, S., Ganesan, S., Murthy, O.V.R. and Dhall A. (2017): 'Thermal Imaging Based Elderly Fall Detection', in: C. S. Chen, J. Lu and K. K. Ma (eds): *Computer Vision – ACCV 2016 Workshops. ACCV 2016. Lecture Notes in Computer Science*, vol 10118, Springer, Cham., doi.org/10.1007/978-3-319-54526-4_40

Yang, D., Chae, Y-J., Kim, D., Lim, Y., Kim, D. H., Kim, C. H., Park, S-K., and Nam, C. (2022): Effects of Social Behaviors of Robots in Privacy-Sensitive Situations, International Journal of Social Robotics, vol. 14, no. 294, July 2021, pp. 589-602, https://doi-org.ezproxy.uio.no/10.1007/s12369-021-00809-2

Yang, G-Z., Nelson, B. J., Murphy, R. R. et al (2020): 'Combating COVID-19 — The role of robotics in managing public health and infectious diseases', *Science Robotics*, vol. 5, issue 40, March 2020, doi.org/10.1126/scirobotics.abb5589

Zoltán Alexin (2022): Entropy based approach to personal data. In: Proceedings of the International Conference on Privacy-friendly and Trustworthy Technology for Society – COST Action CA19121 - Network on Privacy-Aware Audio- and Video-Based Applications for Active and Assisted Living

Entropy based approach to personal data

Zoltán Alexin
University of Szeged, Department of Software Engineering, Hungary
alexin@inf.u-szeged.hu

Abstract

The forthcoming decade is envisioned being the era of Artificial Intelligence (AI). It seems that everything is at the disposal of the industry: the computing power, the large storage, and the Big Data. The latter is a key component of the AI systems, because the researchers' community considers that more training data result in more accurate AI software. Therefore, the industries demand larger and larger amount of genetic, biometric, health, geolocation, travel, and financial etc. data. The European Union and the member states try to keep the pace dictating the US and China and tend to satisfy the needs of the industries by laws, like the European Health Data Space (EHDS) Regulation, the AI Regulation. Applying these laws, the industries can get the much-needed data for themselves. What remains unsolved although, is the protection of individuals with regard to the automatic processing of personal data relating to them.

The requested data many times are personal data, at least once they were personal. Then underwent a de-identification procedure by which the natural identifiers were deleted. But it is not enough, because the data may still contain so-called quasi-identifiers by which an adversary can join two completely different datasets together and reveal the identity of the individuals whom the data relates to. When we talk about joining, it many times is understood in the general sense. That means, it can be executed based on proximity in time or geolocation, not only on the basis of identical values of some quasi-identifiers.

The author proposes a statistical method by which data protection experts can investigate datasets before handing over them to the industries. The method provides one single number, an entropy value, characteristic to the dataset that shows its vulnerability against re-identification attacks. The side effect of the method is that it provides distribution data over the quasi-identifiers, by which the analysts can identify the most and least vulnerable part of the population. The biggest risk is an adversary has a nationwide other dataset to attack with. To arm ourselves, we can model this kind of situation too by studying the entropy values and the distribution of quasi-identifiers at national level.

Introduction

Since the protection of personal data became a fundamental right in the European Union in 2009, when all member states undersigned the TFEU (Lisbon Treaty), it was always a question how we can decide that a particular dataset is personal at all. The law protects only personal data therefore such a judgement is crucial when a company, clinics or a public institution etc. want to share or publicize a dataset. In the case of health data, the rules of professional ethics also prohibit to reveal personal medical information before others.

The GDPR proposed a mean, by which the privacy rights of individuals can eventually be protected. It is the anonymization. The term assumes that the result of the process is an anonymous dataset. Since anonymity is questionable sometimes, therefore the *de-identification* is a more correct term. This latter means that the process intends to render the data anonymous, but it is not sure that this goal is achieved. Many cases were reported in the literature, for example in (Ohm, 2010) where the allegedly anonymous data later have been broken. This shows that the decision on anonymity must be especially cautious and be based on strong statistical evidence. The HIPAA law (US Federal Government, 2022) for example contains that a covered entity may determine that health information is not individually identifiable health information only if:

> § 164.514 b) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:
>
> (i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and
>
> (ii) Documents the methods and results of the analysis that justify such determination

Such type of legal regulation is not known in the EU. According to the GDPR, the Data Protection Officer, who is generally a lawyer will decide on the anonymity of a dataset. The newly passed Hungarian Act XCI of 2021 on National Data Assets contains this approach too. In (Alexin, 2018) the author presented two court cases filed by himself on medical data protection. In one case the Supreme Court of Hungary after several appeals finally decided that the national Itemized Medical Dataset (IMD) does not contain personal data, although it contains a pseudonym (9-digit number), the birthdate, ZIP code, gender, dates of care, institutions, medicines related with a patient. Consequently, data subjects have no rights to access, to object, to be forgotten.

In (Higgins, 2021) the author argues that careful statistical analysis is essential before a research database is published. Datasets are analyzed from the point of view of k-anonymity and l-diversity. They quantified the risk for three scenarios:

- friendly researcher who might inadvertently reidentify an acquaintance
- a rogue researcher deliberately attempting reidentification using public information, and
- a rogue corporation with wide data access.

The future perspective is rather disappointing. Each day hackers stole a new personal database containing identification data for thousands if not millions of people. These databases sooner or later are being commercialized in the dark net. So, we must prepare for the case when any tiny identifier fragments in a de-identified dataset can be keys for re-identification. Some years ago, the data items in a dataset could be divided into two parts: quasi-identifiers and such type of data that are considered not suitable for re-identification. As hackers can have access to the original databases, we must accommodate to the fact that each data item will become quasi-identifier. In healthcare for example, the Electronic Health Record (EHR) systems holding all medical information from birth to death became a standard, therefore any tiny data item (heart rate, bilirubin concentration in urine, body weigh on a particular date) can be used for re-identification of patients either by an insider adversary (e. g. authority, researcher) or a hacker who stole original data records.

The anonymity therefore depends only on the amount of information about an individual stored in the de-identified dataset. The world population is 7.9 billion which corresponds to 33 bits of information, the population of Hungary is 10 million, it corresponds to 24 bits ($\log_2(population)$). See (Chang, 2019) which is a good attention-grabbing article on the topic. This amount of information is enough to identify somebody given the adversary can get such a personal database (a clue) that contains the complete or identical form of the quasi-identifiers exist in the de-identified dataset.

Computing the entropy of a dataset

In the probability theory a random variable X is a measurable function $X : \Omega \rightarrow E$ from a set of possible outcomes Ω to a measurable space E. In continuous case could be rather difficult but in the following the discrete case is applied. The Ω will denote a population. It can be a whole country, like Hungary, is a finite set. The random variable X randomly select an individual from the population and returns the quasi-identifiers of that individual as a tuple, like $(a, b, c, \dots)$, where $a \epsilon A, b \epsilon B, c \epsilon C$ etc. A could be the set of ZIP codes, where the individuals live, B could be the set of ages, C could be the set of genders. Such a way, $E = A \times B \times C \times \dots$. In our case $A, B, C, \dots$ all finite sets, therefore E also will become finite.

The probability of some $S \subseteq E$ is defined as

$$P(X \epsilon S) = P(\omega \epsilon \Omega : X(\omega) \in S) \tag{1}$$

It is assumed that every individual in the population is equally probable. Then $P(X \epsilon S)$ is proportional with the number of individuals whose quasi-identifiers are in S. Let the number of such individuals be k. S may contain one single element (tuple) from E. The values of P can be narrowed between *0* and *1* by dividing it with the number of elements in Ω. Let the number of elements in Ω *is* N. $|\Omega| = N$.

$$P(X \epsilon S) = \frac{|\{\omega \epsilon \Omega : X(\omega) \in S\}|}{|\Omega|} = \frac{k}{N} \tag{2}$$

This way $P(E) = 1, P(\emptyset) = 0$.

The probabilities of certain quasi-identifiers may differ. For example, the population in two ZIP code districts may differ substantially. If we select citizens fairly and randomly then the probability of choosing someone from a more populated ZIP code district is larger, as suggests formula (2).

Claude Shannon published his well-known formula in (Shannon, 1948) by which one can compute the information content of telecommunication messages.

$$E(Message) = -\sum_{i=1}^{n} P(\{x_i\}) \; log_2 \, P(\{x_i\}) \tag{3}$$

In his formula a $Message$ is composed of letters $x_1, x_2, \dots, x_n$. The probabilities of the letters are given in advance. With the above formula (3) he can determine the information content (entropy) of any message.

In this paper the author proposes a new application of the formula (3). The dataset being inspected is considered a $Message$. We assume that it contains quasi-identifiers of random citizens. The letters will be the quasi-identifiers (tuples). The

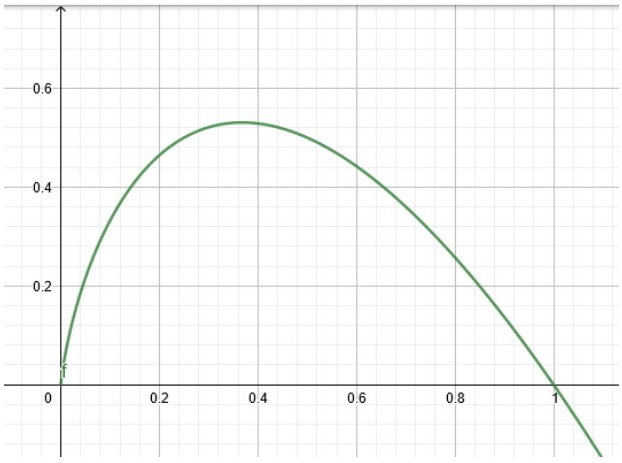
probabilities of the quasi-identifiers can be determined in advance. The best is to obtain data from national offices of statistics, or other official sources that are comprehensive and reliable. The application of the logarithm function can be reasoned as follows. If k individuals from the population share the same quasi-identifier (x_i) such a way that they cannot be distinguished from each other. In this case, the amount of information, the number of bits we can get to know is $\log_2(N/k)$. Because we can determine the group of k individuals having this quasi-identifier but cannot select one individual from the group. The $\log_2(N/k) = -\log_2(k/N) = -\log_2 P(\{x_i\})$.

One important note! In this paper a dataset $\mathcal{D}$ is considered a regular relational dataset, which means that one individual may occur at most once among the records. With this assumption the formula (3) provides a real and interpretable measure of unorderedness (entropy) over the quasi-identifiers of the population. Otherwise, the following considerations may not be true, for example, the amount of information accumulated in the dataset may increase indefinitely.

$$\mathcal{E}(E) = -\sum_{all\ e \epsilon E} P(\{e\})\ log_2 P(\{e\}) \tag{4}$$

On the other hand, when we have a snapshot of quasi-identifiers, we can compute the entropy for the whole population. During the computation a detailed insight to the distribution of the quasi-identifiers is also obtained. The distribution of the information gain can be characterized as well, for example we can tell the probability (number of individuals) of gaining at least n bit information about the individuals for a given n.

Figure I. The graph of the $f(x) = -x \log_2 x$ function



A plot of the function shows, that function $f(x)$ it can be computed only for positive real numbers. When $x = 0.0$ the right limit is 0.0, for $x = 0.25$ and $x = 0.5$ $f(x)$ will be 0.5 in both cases. The maximum $1/(e \ln 2)$ is reached when $x = 1/e$.

The author obtained a statistical research dataset from the population registry. The flowing computations all are demonstrated by this database. The research published here is considered a preliminary investigation.

What increases and decreases the entropy?

Lemma 1

Let N be a fixed integer number (e. g. the population taken), then the following inequality is held for all $0 < i, j, (i + j) < N$ integer numbers:

$$-\frac{i}{N}\log_2\frac{i}{N}-\frac{j}{N}\log_2\frac{j}{N}>-\frac{i+j}{N}\log_2\frac{i+j}{N} \tag{5}$$

Proof
If we substitute $a = i/N$ and $b = j/N$ then $0 < a, b, (a + b) < 1$ we get the following formula:

$$-a\log_2 a - b\log_2 b > -(a+b)\log_2(a+b) \tag{6}$$

which is equivalent

$$-\log_2 a^a b^b > -\log_2(a+b)^{(a+b)} \tag{7}$$

since a and b are positive numbers and less than 1, $1/a > 1/(a+b) > 1$

$$\log_2\left(\frac{1}{a}\right)^a\left(\frac{1}{b}\right)^b > \log_2\left(\frac{1}{a+b}\right)^a\left(\frac{1}{a+b}\right)^b = \log_2\left(\frac{1}{a+b}\right)^{(a+b)} \tag{8}$$

In fact, the inequality is held for all $0 < a, b$ values. If either of them, for example b is greater than 1, then the above formula can be modified as follows:

$$\log_2\left(\frac{1}{a}\right)^a\frac{1}{b^b} > \log_2\left(\frac{1}{a+b}\right)^a\frac{1}{(a+b)^b} = \log_2\left(\frac{1}{a+b}\right)^{(a+b)} \tag{9}$$

From the above lemma it follows for example, that

$$-\frac{1}{N}\log_2\frac{1}{N}-\frac{1}{N}\log_2\frac{1}{N}-\frac{1}{N}\log_2\frac{1}{N}-\frac{1}{N}\log_2\frac{1}{N}>-\frac{4}{N}\log_2\frac{4}{N} \tag{10}$$

$$-k\frac{1}{N}\log_2\frac{1}{N} > -\frac{k}{N}\log_2\frac{k}{N} \tag{11}$$

$$\log_2 N = -N\frac{1}{N}\log_2\frac{1}{N} \geq \sum_{i=1,2,\ldots,n}^{k_1+k_2+\cdots+k_n=N} -\frac{k_i}{N}\log_2\frac{k_i}{N} \tag{12}$$

The formula (12) says that the entropy of any discrete random variable must be less than or equal to $\log_2 N$ where N is the number of elements in Ω. The maximum value is reached if all individuals have different quasi-identifiers. In Hungary $\log_2(N)$ is ~23.254 bits. The formula (12) will result in 0, if all individuals belong to one single group of N indistinguishable individuals.

Lemma 2

The following inequality (13) is held for all $0 < k < l < N$ integer numbers. Having $k \cdot l$ individuals, such that they have l different quasi-identifiers, and for each quasi-identifier there exist exactly k individual who has this quasi-identifier. If we reverse the role of k and l, (k different quasi-identifier and l individual who has it) then the entropy will decrease. That means, the entropy can be decreased if we increase the number of indistinguishable individuals (from k to l).

$$-l\,\frac{k}{N}\log_2\frac{k}{N} > -k\frac{l}{N}\log_2\frac{l}{N} \tag{13}$$

$$-\frac{lk}{N}\log_2\frac{k}{N} > -\frac{kl}{N}\log_2\frac{l}{N} \tag{14}$$

The logarithm function is monotonic increasing, therefore the inequality (15) is held, because $k < l$. If we multiply both sides with the same negative coefficient $-kl/N$, then the direction of the inequality will reverse.

$$\log_2\frac{k}{N} < \log_2\frac{l}{N} \tag{15}$$

Corollary

$$-3\,\frac{3}{N}\log_2\frac{3}{N} > -\frac{4}{N}\log_2\frac{4}{N} - \frac{5}{N}\log_2\frac{5}{N} \tag{16}$$

We have 9 individuals in three groups such that we cannot distinguish them within a group. If we re-arrange them in two groups with 4 and 5 individuals such a way that they cannot be distinguished within a corresponding group, then the entropy will decrease. Lemma 2 is used twice for proving:

$$-4\,\frac{3}{N}\log_2\frac{3}{N} > -3\frac{4}{N}\log_2\frac{4}{N} \tag{17}$$

$$-12\,\frac{3}{N}\log_2\frac{3}{N} > -9\frac{4}{N}\log_2\frac{4}{N} \tag{18}$$

$$-12\,\frac{3}{N}\log_2\frac{3}{N} > -4\frac{4}{N}\log_2\frac{4}{N} - 5\frac{4}{N}\log_2\frac{4}{N} \tag{19}$$

$$-12\,\frac{3}{N}\log_2\frac{3}{N} > -4\frac{4}{N}\log_2\frac{4}{N} - 4\frac{5}{N}\log_2\frac{5}{N} \tag{20}$$

$$-3\,\frac{3}{N}\log_2\frac{3}{N} > -\frac{4}{N}\log_2\frac{4}{N} - \frac{5}{N}\log_2\frac{5}{N} \tag{21}$$

k-anonymity:

A dataset $\mathcal{D}$ is considered k-anonymous for any natural number k, if for all records (representing a natural person) there exist at least $k-1$other record (individual) that they are indistinguishable from each other considering their quasi-identifiers.

Lemma 3

If a dataset $\mathcal{D}$ is k-anonymous then its entropy $\mathcal{E}(\mathcal{D}) < -\log_2(k/N)$, where N is the number of individuals in the dataset.

$$-\log_2\frac{k}{N} \geq \sum_{i=1,2,\ldots,n}^{k_1+k_2+\cdots+k_n=N,\ k_i\geq k} -\frac{k_i}{N}\log_2\frac{k_i}{N} \tag{22}$$

Proof

It follows from the definition of k-anonymity and from Lemma 2. In the trivial case, when have exactly k individuals who share common quasi-identifiers and N is therefore divisible by k. Then we get the following formula:

$$\sum_{i=1,2,\ldots,N/k}^{k+k+\cdots+k=N} -\frac{k}{N}\log_2\frac{k}{N} = \frac{N}{k}\left(-\frac{k}{N}\log_2\frac{k}{N}\right) = -\log_2\frac{k}{N} \tag{23}$$

In general case, by applying Lemma 2 we can bring in new groups with $k+1, k+2, \ldots$ indistinguishable individuals, while doing this the entropy always decreases. A more elaborated formal proof is not available currently. See the Corollary also!

If the entropy of a dataset $\mathcal{D}$ is $\mathcal{E}(\mathcal{D})$, then we can compute an estimated k value, which is characteristic to the anonymity of the dataset.

$$-\log_2 \frac{k}{N} = \mathcal{E}(\mathcal{D}) \tag{24}$$

$$k = \frac{N}{2^{Entropy}} \tag{25}$$

From Lemma 3, it follows that the entropy of a 2-anonymous dataset is less or equal to $-\log_2(2/N) = \log_2(N/2) = \log_2(N) - 1$. An interesting question arose here: if we have a dataset $\mathcal{D}$ and its entropy falls between $\log_2(N) - 1 < \mathcal{E}(\mathcal{D}) < \log_2(N)$ then how many uniquely identifiable records (singletons) must exist in the database? The following equation system needs to be solved.

$$-\lambda_2 \frac{2}{N} \log_2 \frac{2}{N} - \lambda_1 \frac{1}{N} \log_2 \frac{1}{N} = \mathcal{E}(\mathcal{D}) \tag{26.1}$$

$$2\,\lambda_2 + \lambda_1 = N \tag{26.2}$$

By substituting λ_1/N by x the following equation is obtained:

$$(1-x)\,(\log_2(N) - 1) + x \log_2(N) = \mathcal{E}(\mathcal{D}) \tag{27}$$

$$\log_2(N) - 1 + x = \mathcal{E}(\mathcal{D}) \tag{28}$$

$$x = \mathcal{E}(\mathcal{D}) + 1 - \log_2(N) \tag{29}$$

$$\lambda_1 = (\mathcal{E}(\mathcal{D}) - (\log_2(N) - 1)) * N \tag{30}$$

It shows, that if the entropy is less than $\log_2(N) - 1$ then no singletons are guaranteed, but above this threshold the number of guaranteed singletons is increasing until it reaches N when the entropy becomes $\log_2(N)$. The number of singletons can be larger, if the dataset $\mathcal{D}$ contains, not only pairs, but couple of sets of three, four, five, … indistinguishable individuals.

$$n_{singletons} \geq (\mathcal{E}(\mathcal{D}) - (\log_2(N) - 1)) * N \tag{31}$$

The entropy computations with the Hungarian population registry dataset

The author obtained a research dataset from the Central Office for Administrative and Electronic Public Services (in Hungarian: Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala, KEKKH) which contained all Hungarian citizens' date of birth, ZIP code of his/her resident address and gender. Altogether 10 004 090 people were in it, $N = 10\,004\,090$. The dataset is a snapshot which have been taken on 31st December 2011 at midnight. Earlier, in (Alexin, 2014) the author investigated the dataset from the point of view of identifiability.

The **Bits** column is always defined as $\log_2(N/k)$. The value of **Entropy** is: $-k/N \log_2(k/N)$.

The entropy of the ZIP code quasi-identifier

Table I. Hungarian ZIP codes, population, and information content

ZIP code	Settlement	Population	Bits	Entropy
1011	Budapest I.	3286	11,5719	0,003800
1012	Budapest I.	4446	11,1357	0,004948
1013	Budapest I.	3404	11,5210	0,003920
…				
9982	Apátistvánfalva	589	14,0519	0,000827
9983	Szakonyfalu	769	13,6672	0,001050
9985	Felsőszölnök	589	14,0519	0,000827
Sum:		**10004090**		**10,303428**

The result of the computation shows that that the entropy of ZIP codes is 10,3 bits. It means that statistically, for a random citizen the expected amount of information in his/her ZIP code is 10.3 bits. It may be more or less since it is an average. It corresponds to 7916-anonymity using the formula (25). Therefore, the ZIP code alone does not mean any privacy risk in a database.

When we look at the Table II. closely, we see that although, the median is about 10 bits, the amount of information gained form a ZIP code ranges from 6 bits to 15 bits. The reason is that the population in a ZIP code district is rather imbalanced. There are sparsely and densely populated districts. The range is from 100 to 100 000. For 48 593 citizen the ZIP code means 15 bits (305-anonymity). It is an elevated but bearable risk.

Table II. The probability of gaining at least *n* bit information if someone's ZIP code is known

Bits	Population	Probability
15	48593	0,49%
14	302595	3,02%
13	966087	9,66%
12	2139699	21,39%
11	3476436	34,75%
10	5210515	52,08%
9	7369394	73,66%
8	8847670	88,44%
7	9716633	97,13%
6	10004090	100,00%

The entropy of the date of birth quasi-identifier

Table III. Hungarian birthdates' distribution, and their information content

Birthdate	Population	Bits	Entropy
1894.12.31.	1	23,25409	2,32446E-06
…			
1985.01.01.	306	14,996698	0,000458711
1985.01.02.	335	14,866069	0,000497810
1985.01.03.	365	14,742333	0,000537875
1985.01.04.	367	14,734450	0,000540533
1985.01.05.	331	14,883399	0,000492439
1985.01.06.	296	15,044633	0,000445139
…			
Sum:	**10004090**		**14,918582**

In this case the result of the computation shows that that the entropy is 14,918 bits. It corresponds to 323-anonymity using the formula (25). Therefore, the date of birth alone does not mean serious privacy risk in a database. The eldest citizen was born in 1894. according to the dataset. It can be seen, that among those people who was born at the beginning of 1985, usually ca. 300 were indistinguishable.

The distribution of the information gain is more balanced as shown in Table IV. It ranges from 13 to 17 bits. The number of indistinguishable citizens is decreasing year by year, but slowly. The number of births is quite stable and even. From the first line we can discover that in the case of 907 citizen the date of birth means unique identifiability (23 bits, 1-anonymity), for 1979 citizens the gain is 22 bits, 2-anonymity, for 4573 21 bits, 3- or 4-anonymity. The table helps us to recognize that we have a smaller, but vulnerable group of people who needs special attention.

The author computed the entropy of the year and month of birth quasi-identifier which resulted in 9.99 bits, 9837-anonymity. This way the risk can be substantially reduced, but these very old citizens remain still uniquely identifiable. Their data shall be suppressed before transferring.

Table IV. The probability of gaining at least *n* bit information if someone's date of birth is known

Bits	Population	Ratio
23	907	0,01%
22	1979	0,02%
21	4573	0,05%
20	10944	0,11%
19	15778	0,16%
18	38252	0,38%
17	117105	1,17%
16	378792	3,79%
15	3282589	32,81%
14	9994548	99,90%
13	10004090	100,00%

Cartesian products of certain quasi-identifiers

Table V. Hungarian $Birthdate \times ZIP\ code$ distribution and the information content

Birthdate x ZIP code	Population	Bits	Entropy
(1894.12.31., 3744)	1	23,254	2,324458e-6
…			
(1975.08.04., 9400)	4	21,254	8,498159e-6
(1975.08.04., 9407)	1	23,254	2,324458e-6
(1975.08.04., 9473)	1	23,254	2,324458e-6
(1975.08.04., 9523)	1	23,254	2,324458e-6
(1975.08.04., 9600)	1	23,254	2,324458e-6
(1975.08.04., 9700)	6	20,669	1,239640e-5
…			
Sum:	**10004090**		**22,79385**

The result of the computation shows dramatic changes when we examine the date of birth x ZIP code quasi-identifier. See Table V. The entropy became 22,7985 bits. It corresponds to 1.37-anonymity using the formula (25). This database poses substantial risk for re-identification. Must not be released or transferred. Using the formula (31) the ratio of singletons is greater the 54% of the population, in fact it was 6635838 individuals. This is clearly seen in Table VI.

Table VI. The probability of gaining at least *n* bit information if someone's date of birth and ZIP code are known

Bits	Population	Ratio
23	6635838	66,33%
22	8629982	86,26%
21	9692881	96,89%
20	9996707	99,93%
19	10004090	100,00%

Table VII. Hungarian $birthdate \times ZIP\ code \times Gender$ distribution and the information content (M – male, F – female)

Birthdate x ZIP x gender	Population	Bits	Entropy
(1894.12.31., 3744, M)	1	23,254	2,324458e-6
…			
(1954.04.14., 6000, M)	1	23,254	2,324458e-6
(1954.04.14., 6041, M)	1	23,254	2,324458e-6
(1954.04.14., 6066, M)	2	22,254	4,448998e-6
(1954.04.14., 6070, F)	1	23,254	2,324458e-6
(1954.04.14., 6097, F)	1	23,254	2,324458e-6
(1954.04.14., 6097, M)	1	23,254	2,324458e-6
…			
Sum:	**10004090**		**22,992721**

The last computation shows even dramatic changes when we examine the date of birth x ZIP code x gender quasi-identifier. See Table VII. The entropy became 22,9927 bits. It corresponds to 1.19-anonymity using the formula (25). This database poses substantial risk for re-identification. Using the formula (31) the ratio of singletons is greater the 74% of the population, in fact it was 7845850 individuals. This is seen in Table VIII.

Table VIII. The probability of gaining at least *n* bit information if someone's date of birth and ZIP code and gender are known

Bits	Population	Ratio
23	7845850	78,43%
22	9403904	94,00%
21	9942428	99,38%
20	10003959	99,99%
19	10004090	100,00%

Summary

This article presented preliminary research on the entropy of certain quasi-identifiers, and combination of quasi-identifiers based on reliable statistical data. The computations can be repeated by other national databases with other quasi-identifiers. The presented approach could be an ultimate decision-support tool for data guardians before they decide on the transfer of a dataset to third parties.

Acknowledgments

The author wishes to thank for the support of the COST Action CA19121 Network on Privacy-Aware Audio- and Video-Based Applications for Active and Assisted Living *"GoodBrother"* project.

The author would like to express his thanks to the Central Office for Administrative and Electronic Public Services (in Hungarian: Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala, KEKKH) for the research dataset extracted from the national population registry.

References

Alexin, Z. (2014): Does fair anonymization exist? International Review of Law, Computers and Technology, Taylor & Francis Publishing, Vol. 28 No. 1: pp. 21-44, DOI: 10.1080/13600869.2013.869909

Alexin, Z. (2018): Court cases relating to medical data protection, Interdiszciplináris Magyar Egészségügy, Larix Kiadó Kft., in Hungarian, Vol.: XVII. No.:3, pp. 57-62

Chang, Kenny (2019): Personal Data and 33 bits of Entropy, SynchLab webpage: https://synch.law/personal-data-and-33-bits-of-entropy/

Ohm, P. (2010). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization UCLA Law Review, University of Colorado, Law Legal Studies Research Paper Vol. 57, No. 9-12, p. 1701, Available at SSRN: https://ssrn.com/abstract=1450006

Shannon, C. E. (1948). A mathematical theory of communication. Bell System Technical Journal. 27 (3): 379–423, 623–656. doi:10.1002/j.1538-7305.1948.tb01338.x.

Sweeney, L. (2000) Simple demographics often identify people uniquely, Data Privacy Working Paper 3. Pittsburgh Carnegie Mellon University, http://dataprivacylab.org/projects/identifiability/paper1.pdf

Higgins T. L. (2021): Reidentification of Protected Health Information: Can the Risk Be Quantified? Crit Care Med. 2021 Jun 1;49(6):1003-1006. doi: 10.1097/CCM.0000000000004931. PMID: 34011836.

US Federal Government (2022). 45 CFR 164.514 Other requirements relating to uses and disclosures of protected health information (HIPAA Law, The privacy rule). https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-E

Palmer, A.; Perez-Vega, R.; Zhang, R., and Scher-Smith, A. (2022): Service Robotics Beyond Privacy Concerns: An Investigation of the Role of Learning Abilities on Technological Adoption. In: Proceedings of the International Conference on Privacy-friendly and Trustworthy Technology for Society – COST Action CA19121 - Network on Privacy-Aware Audio- and Video-Based Applications for Active and Assisted Living.

Service Robotics Beyond Privacy Concerns: An Investigation of the Role of Learning Abilities on Technological Adoption

Adrian Palmer[1], Rodrigo Perez-Vega[2], Ruby Zhang[1] and Alex Scher-Smith[1]
[1]Henley Business School, University of Reading, [2]Kent Business School, University of Kent.
a.palmer@henley.ac.uk, R.Perez-Vega@kent.ac.uk, ruby.zhang@henley.ac.uk, a.scher-smith2@henley.ac.uk

The rapid expansion of AI technology has led service robotics to become an increasingly adopted tool to complement and reduce human inputs in diverse service sector settings (Bohr and Memarzadeh, 2020; Chiang and Trimi 2020; Fosch-Villaronga and Drukarch, 2021). In this paper, we investigate their application in the context of personal care services. We specifically contribute to knowledge in the domain by investigating the effects of consumers' learning style on their adoption of AI assisted technologies and on implications for consumers' privacy.

Prior research into service robotics, has identified a long list of challenges that need further investigation from the perspectives of privacy, security, financial risk, product risk and information risk (Lenca and Villaronga, 2019; Bhatnagar et al.,

2000; Tsu et al., 2009; Dinev and Hart, 2006). In the context of robotic care assistants, there are divided views ranging from fear to awe, with research currently emphasising a perspective that users prefer to use an anthropomorphic robot due to a high degree of empathy (Akdim et al., 2021; Christou et al., 2020; Tussyadiah & Park, 2018). More generally within service sectors, especially the educational and hospitality sectors (Paluch et al., 2020), it has been noted that humanoid robots can evoke insecurity and negative responses. Security concerns are a prominent issue with consumers still showing a reluctance to accept Intelligent Assistive Technologies (IATs), primarily due to privacy concerns (Lutz, and Tamo-Larriuex, 2020; Lenca and Villaronga, 2019; Pavlou, 2001), and therefore, the perceived risk of adopting these new technologies emerges as a prominent barrier to consumer acceptance of advanced robotics. Furthermore, Jia et al. (2021) studied the complexities of human-likeness of robots within the hotel sector and found individuals are less receptive towards anthropomorphic robots due to safety and simulation of human behaviours. Previous studies provide contradictory findings and indicate the complexities of consumer behaviours with novel robotic technologies across the education and travel & tourism sectors (Chuah et al., 2021). However, little is known about how consumers evaluate new technologies for potential adoption and how they learn these new technologies through picking out moments associated with prior experiences. A better understanding of how service robots can be used to connect families, provide ongoing support from hospitals to residential environments and achieve acceptance rates over assistive technologies is an important social issue (Bogue, 2020; Murphy et al., 2020; Seyitoglu and Ivanov, 2020).

Bauer (1960) was an early scholar to associate perceived risks with consumer behaviour. A definition of perceived risk within the context of electronic commerce is given by Pavlou (2003), as "the user's subjective expectation of suffering a loss in pursuit of a desired outcome". Siau and Shen (2003) point out that both security and privacy risk are part of the essential factors that hinder user acceptance. Tsu et al. (2009) agreed that both security and privacy influence consumers' decisions to use new forms of technology. With the purpose of focusing on consumers' privacy concerns and use of new technology context, the UTAUT2 model is thus adapted as the underpinning theoretical framework of this research. A theoretically and empirically important aim of this study is to clarify the constructs that internally affect the acceptance and behaviours of consumers for service robotics adoption, and other future potential innovations. Therefore, insights of individual's cognitive and affective learning ability are studied in order to identify how the learning styles of consumers have impacted the adoption of new technologies across consumer's acceptance and behaviours. The way consumers learn and structure information is a strategic concern for business practice in the context of implementation of service robots.

Methodological Approach

This research aims to investigate consumers' acceptance and behavioural intention of new technologies in the UK, with a specific focus upon service robotics and privacy. Additionally, as service robotics are still novel in many countries, including the UK, insights into behavioural intentions are limited and a general population sample garners wider insight. Thus, the target population of this quantitative study is focused on adult consumers residing in the UK regardless of gender, marital status, education level and other background contexts. This study used online data collection, which incorporated panel data for the purpose of aiding University research studies and rewards participants with a fee for their participation. More researchers in the social sciences domain are turning to online panel data collections for research purposes (Lovett et al., 2018). To achieve the objectives of this study, an analytical framework is constructed for deriving factors for the prediction of an individual's acceptance and behavioural intention of service robotics. Furthermore, this research implemented a quantitative questionnaire, with 400 completed responses. Thereafter, the quantitative analysis was conducted using SPSS and SmartPLS 3.0 software on the basis of the Structural Equation Modelling technique (SEM). After a thorough review of literature and studies related to the UTAUT and UTAUT2 model, the instruments were developed accordingly. Six key constructs were adopted from the second generation of the UTAUT2 model (Venkatesh et al., 2012). The items for measuring utilitarian motivation in this research were partially adopted from Babin et al. (1994) and Kim (2006); four relevant items of the TRI scale were selected in this study for technology readiness due to the length of the measurement (Parasuraman, 2000; Liljander et al., 2006); seven measurement items were adapted from Featherman and Pavlou (2003), reflecting the perception of seven dimensions of risk with the focus of privacy risk; The Acceptance of Change Scale (ACS) was adapted to examine the tendency of individuals to accept or move toward change (Di Fabio and Gori, 2016). To measure consumer cognitive learning ability, three measuring items of the Need for Cognition Scale (NCS) and three measuring items of the Cognitive Load Questionnaire (CLQ) were adapted for this research. As for affective learning ability, this research adapted from the research from McCroskey (1994) and Mottet and Richmond (1998) and, nonetheless, modified the wordings to keep a consistency with other statements in a service robotic context.

Findings

We show that the relationship between utilitarian motivation and intention of acceptance of service robots is mediated by the degree of performance expectancy, and has no direct relationship with effort expectancy. A similar relationship was found for technology readiness and perceived risk. For both antecedents, the relationship with intention of acceptance is also mediated by performance expectancy. We also found a direct relationship between perceived risk and

intention of acceptance. The implication of these findings suggests that understanding the expectations consumers have of these robots to perform different tasks is central to the intention to adopt service robot technologies. Furthermore, in terms of the moderating role of learning abilities, our findings suggest that there is a significantly negative moderation effect of cognitive learning ability on the relationship between utilitarian motivation and performance expectancy. In other words, for those consumers who have lower cognitive learning ability, utilitarian motivation positively affects their performance expectancy more than those with higher cognitive learning ability. Furthermore, affective learning ability has a positive moderation effect on the relationship between technology readiness and performance expectancy. Therefore, for those consumers who have higher affective learning ability, technology readiness positively affects their performance expectancy more than those with lower affective learning ability. Due to the crucial role that performance expectancy has as a mediator in the adoption of service robots, tailoring the features that allow service robots to perform tasks based on the learning ability of the user can facilitate further the intentions to adopt them.

References

Akdim, K, Belanche, D and Flavián, M. (2021). Attitudes toward service robots: analyses of explicit and implicit attitudes based on anthropomorphism and construal level theory. International Journal of Contemporary Hospitality Management. Spain. 10.1108/IJCHM-12-2020-1406.

Babin, B. J., Darden, W. R., and Griffin, M. (1994). Work and/or Fun: Measuring Hedonic and Utilitarian Shopping Value. The Journal of Consumer Research, 20, (4). Oxford. 644-656.

Bauer, R.A. (1960) Consumer Behavior as Risk Taking. In: Hancock, R.S., Ed., Dynamic Marketing for a Changing World, Proceedings of the 43rd. Conference of the American Marketing Association, 389-398.

Belanche, D, Casaló, V.L, Flavián, C, and Schepers, J (2020). Service robot implementation: a theoretical framework and research agenda, The Service Industries Journal, 40, 3-4, 203-225, DOI: 10.1080/02642069.2019.1672666.

Bhatnagar, A., Misra, S. and Rao, H. (2000). On risk, convenience, and Internet shopping behavior. Communications of the ACM, 43, (11), pp.98-105.

Bohr A, Memarzadeh K. The rise of artificial intelligence in healthcare applications. Artificial Intelligence in Healthcare. 2020;25-60. doi:10.1016/B978-0-12-818438-7.00002-2.

Bougue, R. (2011). Robots in healthcare. Industrial Robot: An International Journal 38: 218-223.

Brooks (Eds.). 1994 SCA summer conference proceedings and prepared remarks, (pp. 55-71). Annandale, VA: Speech Communication Association.

Chiang, AH., Trimi, S. (2020). Impacts of service robots on service quality. Service Bussiness. 14, 439–459. https://doi.org/10.1007/s11628-020-00423-8.

Christou, P, Simillidou, A and Stylianou, M, C. (2020). Tourists' perceptions regarding the use of anthropomorphic robots in tourism and hospitality. International Journal of Contemporary Hospitality Management. ISSN 0959-6119.

Chuah, W-H, S., Aw, X-C, E and Yee, D. (2021). Unveiling the complexity of consumers' intention to use service robots: An fsQCA approach. Computers in Human Behavior 123, 106870.

Di Fabio A., Gori A., Giannini M. (2016). Analysing the psychometric properties of a Big Five measure with an alternative method: The example of the Ten Item Personality Inventory (TIPI). Couns. G. Ital. Ric. Appl. Retrieved from: http://rivistedigitali.erickson.it/counseling/.

Dinev, T, and Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. Information Systems Research. 17. 61-80. 10.1287/isre.1060.0080.

Featherman, M. and Pavlou, P. (2003). Predicting e-services adoption: a perceived risk facets perspective. International Journal of Human-Computer Studies 59, 451-474.

Fosch-Villaronga, E., & Drukarch, H. (2021). On Healthcare Robots. Lieden, the Netherlands: Leiden University. Retrieved from https://arxiv.org/pdf/2106.03468.pdf.

Jarvenpaa, S., Tractinsky, N., & Saarinen, L. (2006). Consumer Trust in an Internet Store: A Cross-Cultural Validation. Journal Of Computer-Mediated Communication, 5, (2), 0-0. doi: 10.1111/j.1083-6101.1999.tb00337.

Jia, J, Chung, N, and Hwang, J. (2021). Assessing the hotel service robot interaction on tourists' behaviour: the role of anthropomorphism. Industrial Management & Data Systems. ahead-of-print. 10.1108/IMDS-11-2020-0664.

Kim, H.S. (2006). "Using Hedonic and Utilitarian Shopping Motivations to Profile Inner City Consumers". Journal of Shopping Center Research, Vol. 13, No. 1, pp. 57-79.

Lenca, M, and Fosch-Villaronga, E. (2019). Privacy and Security Issues in Intelligent Assistive Technologies for Dementia: The Case of Ambient Assisted Living, Wearables and Service Robotics. 10.1093/med/9780190459802.003.0013.

Liljander, V. (2006). Technology readiness and the evaluation and adoption of self-service technologies. Journal of Retailing and Consumer Services 13, 177-191.

Lovett, M., Bajaba, S., Lovett, M. and Simmering, M. (2018). Data Quality from Crowdsourced Surveys: A Mixed Method Inquiry into Perceptions of Amazon's Mechanical Turk Masters. Applied Psychology. 67 (2). pp. 339-366.

Lutz, C., & Tamó-Larrieux, A. (2020). The Robot Privacy Paradox: Understanding How Privacy Concerns Shape Intentions to Use Social Robots. Human-Machine Communication, 1, 87-111. doi: 10.30658/hmc.1.6.

McCroskey, J. C. (1994). Assessment of affect toward communication and affect toward instruction in communication.In S. Morreale and M.

McLeay, F., Osburg, V. S., Yoganathan, V., & Patterson, A. (2021). Replaced by a Robot: Service Implications in the Age of the Machine. Journal of Service Research, 24(1), 104–121. https://doi.org/10.1177/1094670520933354

Mottet, T. and Richmond, V. (1998). Newer is not necessarily better a reexamination of affective learning measurement. Communication Research Reports 15:370-378.

Murphy RR, Gandudi VBM and Adams J. (2020). Robots are playing many roles in the coronavirus crisis—And offering lessons for future disasters. Government Technology. Available at: https://www.govtech.com/products/Robots-Are-Playing- Many-Roles-in-the-Coronavirus-Crisis–and-Offering- Lessons-for-Future-Disasters.html.

Paluch, S, Wirtz, J and Kunz, W. (2020). Service Robots and the Future of Services. 10.1007/978-3-658-31563-4.

Parasuraman, A. (2000). Technology Readiness Index (TRI). Journal of Service Research 2:307-320.

Parasuraman, A. and Colby, C. (2014). An Updated and Streamlined Technology Readiness Index. Journal of Service Research 18:59-74.

Park, Sangwon. (2020). Multifaceted trust in tourism service robots. Annals of Tourism Research. 81. 102888. 10.1016/j.annals.2020.102888.

Pavlou, P. (2001). Integrating trust in electronic commerce with the technology acceptance model: model development and validation. Boston.

Seyitoglu F and Ivanov S. (2020). Service robots as a tool for physical distancing in tourism. Current Issues in Tourism (in press). DOI: 10.1080/13683500.2020.1774518.

Shishehgar, M., Kerr, D., & Blake, J. (2017). The effectiveness of various robotic technologies in assisting older adults. Health Informatics Journal, 25(3), 892-918. doi: 10.1177/1460458217729729.

Siau, K. and Shen, Z. (2003). Building customer trust in mobile commerce. Communications of the ACM, 46(4), pp.91-94.

Tsu Wei, T., Marthandan, G., Yee-Loong Chong, A., Ooi, K. and Arumugam, S. (2009).

What drives Malaysian m-commerce adoption? An empirical analysis. Industrial Management & Data Systems, 109(3), pp.370-388.

Tussyadiah, I and Park, S. (2018). Consumer Evaluation of Hotel Service Robots. 10.1007/978-3-319-72923-7_24.

Venkatesh, Thong and Xu. (2012). Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology. MIS Quarterly 36:157.

Venkatesh, V., Morris, M., Davis., G and Davis, F. (2003). User Acceptance of Information Technology: Toward a Unified View. MIS Quarterly 27:425.

Ross Cheung, Shreshtha Jolly, Manoj Vimal, Hie Lim Kim, and Ian McGonigle (2022): Who's afraid of genetic tests?: An assessment of Singapore's public attitudes and changes in attitudes after taking a genetic test. In: Proceedings of the International Conference on Privacy-friendly and Trustworthy Technology for Society – COST Action CA19121 - Network on Privacy-Aware Audio- and Video-Based Applications for Active and Assisted Living

Who's afraid of genetic tests?: An assessment of Singapore's public attitudes and changes in attitudes after taking a genetic test

Ross Cheung, Shreshtha Jolly, Manoj Vimal, Hie Lim Kim, and Ian McGonigle
Nanyang Technological University, Singapore
s200117@e.ntu.edu.sg, joll0001@e.ntu.edu.sg, vimal.manoj@ntu.edu.sg, hlkim@ntu.edu.sg, ianmcgonigle@ntu.edu.sg

Megarry, J., Kao, Y., Mitchell, P. and Rittenbruch, M. (2022): Probing for Privacy: A Digital Cultural Probe to Support Reflection on Situated Geoprivacy and Trust. In: Proceedings of the International Conference on Privacy-friendly and Trustworthy Technology for Society – COST Action CA19121 - Network on Privacy-Aware Audio- and Video-Based Applications for Active and Assisted Living

Probing for Privacy: A Digital Cultural Probe to Support Reflection on Situated Geoprivacy and Trust

Jessica Megarry
Digital Media Research Centre, Queensland University of Technology
jessica.megarry@qut.edu.au

Yu Kao
QUT Design Lab, Queensland University of Technology
y2.kao@qut.edu.au

Peta Mitchell
Digital Media Research Centre, Queensland University of Technology
peta.mitchell@qut.edu.au

Markus Rittenbruch
QUT Design Lab, Queensland University of Technology
m.rittenbruch@qut.edu.au

Abstract

In this paper, we report on a digital cultural probe study as a method for testing sensitivity to contextual integrity and situated privacy in relation to location-data sharing through digital media. In recent years, (geo)location has emerged as a focal point for discourse and debate about privacy and trust. As smartphone penetration

approaches saturation point in the Global North, an app and data economy built on and monetizing the locative affordances of mobile media has emerged. This rise of ubiquitous geolocation has led researchers to identify location as a uniquely sensitive datapoint and to frame *geo*privacy as an emergent form of situated—and highly situational—privacy requiring critical attention (Leszczynski, 2017; Keßler & McKenzie, 2018; Martin & Nissenbaum, 2020). Alongside this, a strand of research has also addressed geolocation's role as a "technology of trust" (Withers, 2018; Leszczynski & Mitchell 2019) that assembles particular affects of trust to incentivise ongoing engagement with and through digital media.

These intersecting concerns about geolocation, privacy, and trust can be seen in the ways that smartphone manufacturers and providers of mobile operating systems have progressively improved end-user location privacy controls year on year. On any major mobile operating system, location-sharing requires user consent; however, the scale and complexity of data being used and shared among differing parties means that is more challenging than ever for end-users to fully understand the privacy risks, benefits, and implications involved in sharing their location with and through their device. As a result, as research has shown, many smartphone users default to giving consent when they receive notifications asking to allow or disallow location sharing, with the conveniences of sharing location data often overriding the perceived risks (Atteneder & Collini-Nocker, 2018; Riedlinger, Chapman, & Mitchell, 2019; Dobson & Herbert, 2021).

Complicating this further is the fact that privacy—and particularly *geo*privacy—is highly situational, and user concerns about sharing location may change depending on *what* is shared, *why* it is being shared, *who* it is being sharing with, *how* it is being shared, and, importantly *where* and *when* it is being shared. Moreover, whether we feel our privacy has been protected or violated often depends on our roles, relationships, power structures, norms, and internal values (including the goal and purpose of geo-locative data). Building on contextual integrity and privacy regulation theories (Langheinrich, 2001; Nissenbaum, 2004), we understand the concerns people have when they encounter these location-sharing decision points and privacy paradoxes can vary from person to person and even from scenario to scenario.

To respond to the privacy challenges outlined above, and to explore the situated and situational nature of geoprivacy and trust in geolocation, we conducted a study to understand how people interpret location-based data privacy in different situations and contexts. Aiming to explore how different situations, locations and contexts influence the way people intellectually and emotionally respond to privacy decisions, we adopted a cultural probe research method to explore geoprivacy (location-based privacy) and trust in situ. Our goal was to gain an in-depth understanding of situated privacy needs in order to inform the broader discussion of designing for data privacy.

The cultural probes approach is a prominent research method in the field of Human-Computer Interaction and Interaction Design. Cultural probes were initially developed by Gaver et al (1999) as a design-oriented method to acquire

glimpses of people's lives. Gaver et al's (1999) original probe package consists of maps, postcards, a disposable camera and other materials to encourage critical reflection. More recently, studies have used the term "technology probe" to describe cultural probes that incorporate "simple, flexible, [and] adaptable" technologies (Hutchinson et al., 2003) as a design inspiration or as prototypes to allow people to envision how these new technologies may be integrated in their life. Relevant to this study, Boucher et al. (2019) developed ProbeTools, which integrate digital components into the original concept of cultural probes. ProbeTools were designed to offer configurable and "unconventional" digital devices that would enable study participants to engage independently with the research inquiry in their everyday life in creative and playful ways.

The cultural probes approach values play and exploration as ways to engage with research participants (Gaver et al., 2004) and emphasises tangibility through physical engagement with digital and/or analogue artefacts. Privacy research has also engaged to some extent with these concepts of playfulness and tangibility. In privacy studies, the concept of playfulness has been used to carry out privacy training (Dincelli & Chengalur-Smith, 2020) or to influence participants' privacy decision-making (Shklovski & Grönvall, 2020; Shklovski et al., 2014). Where privacy studies has incorporated or focused on tangibility, the tangible technology employed has tended to take the form of a physical interface to manage privacy settings (see, e.g., Ahmad et al., 2020; Jedrzejczyk et al., 2010; Mehta, 2019; Mehta et al., 2021).

In our study, we developed a self-contained digital cultural probe that closely aligns with the ProbeTools concept. We named our probe TamaGeochi (pictured below in fig. 1), referencing the "digital pet" toy Tamagotchi to highlight the probe's physical and playful qualities and incorporating the term "geo" to highlight its focus on location. TamaGeochi's personality was designed to be naïve, curious, and childlike. The device prompted provocative questions about location-based privacy and encouraged participants to reflect on their situated response to privacy by eliciting photos, drawings, and written reflections alongside location data sharing (see fig. 2).

In our paper, we introduce the design elements and research implementation of the TamaGeochi probe and report on the findings from our study, particularly the ways in which TamaGeochi increased awareness of—and self-reflection in relation to—the meaning of location, location tracking technologies, and individual in-situ privacy concerns. We also discuss how trust figured in our participants' responses, highlighting their often contradictory and mercurial feelings about experiences of sharing and tracking in the geodata economy. Finally, we offer insights from a follow up co-design workshop in which our participants were invited to imagine the future of geoprivacy and trustworthy design.

Figure 1

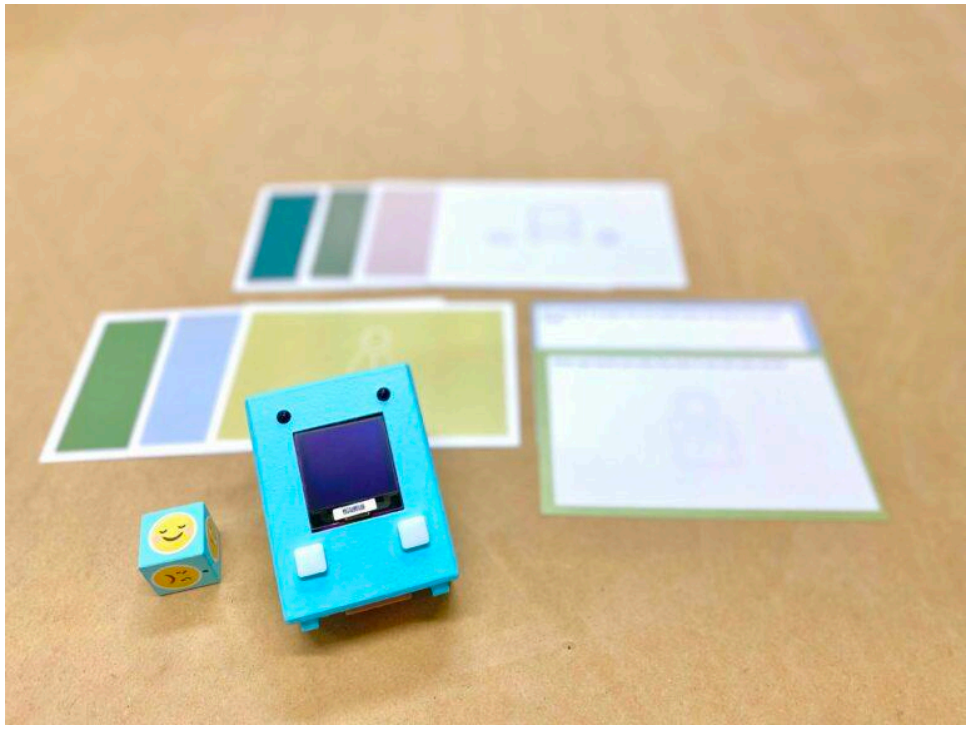


Figure 2

References

Ahmad, I., Farzan, R., Kapadia, A. and Lee, A. J. (2020). 'Tangible privacy: Towards user-centric sensor designs for bystander privacy', *Proceedings of the ACM on Human-Computer Interaction*, vol. 4, no. CSCW2, pp.1–28.

Atteneder, H. and Collini-Nocker, B. (2018). 'Geomedia and privacy in context. Paradoxical behavior or the unwitting sharing of geodata with digital platforms?', *Mediatization Studies*, vol. 2. https://doi.org/10.17951/ms.2018.2.17-48

Boucher, A., Brown, D., Gaver, B., Matsuda, N., Ovalle, L., Sheen, A. and Vanis, M. (2019). 'ProbeTools: Unconventional cameras and audio devices for user research', *Interactions*, vol. 26, no. 2, pp.26–35.

Dincelli, E. and Chengalur-Smith, I. (2020). 'Choose your own training adventure: Designing a gamified SETA artefact for improving information security and privacy through interactive storytelling', *European Journal of Information Systems*, vol. 29, no. 6, pp. 669–687.

Dobson, J.E. and Herbert, W.A. (2021). 'Geoprivacy, Convenience, and the Pursuit of Anonymity in Digital Cities', in Wenzhong Shi et al. (eds.): *Urban Informatics.* Springer, Singapore, 2021, pp. 567-587. https://doi.org/10.1007/978-981-15-8983-6_32

Gaver, B., Dunne, T. and Pacenti, E. (1999). 'Design: Cultural probes', *Interactions*, vol. 6, no. 1, pp. 21–29.

Gaver, W. W., Boucher, A., Pennington, S. and Walker, B. (2004). 'Cultural probes and the value of uncertainty', *Interactions*, vol. 11, no. 5, pp. 53–56.

Hutchinson, H., Mackay, W., Westerlund, B., Bederson, B.B., Druin, A., Plaisant, C., Beaudouin-Lafon, M., Conversy, S., Evans, H., Hansen, H., Roussel, N. and Eiderbäck, B. (2003). 'Technology probes: Inspiring design for and with families', *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 17–24. https://doi.org/10.1145/642611.642616

Jedrzejczyk, L., Price, B. A., Bandara, A. and Nuseibeh, B. (2010). '"Privacy-shake": A haptic interface for managing privacy settings in mobile location sharing applications', *Proceedings of the 12th International Conference on Human Computer Interaction with Mobile Devices and Services*, pp. 411–412.

Keßler, C and McKenzie, G. (2018). 'A geoprivacy manifesto', *Transactions in GIS* 22, pp. 3–19. https://doi.org/10.1111/tgis.12305

Langheinrich, M. (2001). 'Privacy by design — Principles of privacy-aware ubiquitous systems', *Ubicomp 2001: Ubiquitous Computing*, pp. 273–291.

Leszczynski, A. (2017). 'Geoprivacy', in R. Kitchin, T.P. Lauriault and M.W. Wilson (eds.) *Understanding Spatial Media.* Los Angeles: Sage, 2017. pp. 235–244.

Leszczynski, A. and Mitchell, P. (2019). 'Geolocation, trust, and platform affects', *AoIR Selected Papers of Internet Research, 2019*. https://doi.org/10.5210/spir.v2019i0.10940

Martin, K., and Nissenbaum, H. (2020). 'What Is It about Location?', *Berkeley Technology Law Journal*, vol. 35, no. 1, pp. 251–326.

Mehta, V. (2019). ‘Tangible interactions for privacy management’, *Proceedings of the Thirteenth International Conference on Tangible, Embedded, and Embodied Interaction*, pp. 723–726.

Mehta, V., Bandara, A. K., Price, B. A., Nuseibeh, B. and Gooch, D. (2021). ‘Up close & personal: Exploring user-preferred image schemas for intuitive privacy awareness and control’, *Fifteenth International Conference on Tangible, Embedded, and Embodied Interaction*, pp.1–13.

Nissenbaum, H. (2004). ‘Privacy as contextual integrity’, *Washington Law Review*, vol. 79, no. 1, pp. 119–158.

Riedlinger, M., Chapman, C. and Mitchell, P. (2019) ‘Location awareness and geodata sharing practices of Australian smartphone users’, *QUT Digital Media Research Centre*, Australia.

Shklovski, I. and Grönvall, E. (2020). ‘CreepyLeaks: Participatory speculation through demos’, *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society*, pp. 1–12.

Shklovski, I., Mainwaring, S. D., Skúladóttir, H. H. and Borgthorsson, H. (2014). ‘Leakiness and creepiness in app space: Perceptions of privacy and mobile app use’, *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 2347–2356.

Withers, C. W. J. (2018). ‘Trust – in geography’, *Progress in Human Geography* vol. 42, no. 4, pp. 489–508. https://doi.org/10.1177/0309132516688078

Acknowledgments

This research was funded by an Australian Research Council (ARC) Discovery Projects grant (DP180100174).

Alain Sandoz, and Léa Stiefel (2022): Trust vs. control: the dilemma between data distribution and centralization. In: Proceedings of the International Conference on Privacy-friendly and Trustworthy Technology for Society – COST Action CA19121 - Network on Privacy-Aware Audio- and Video-Based Applications for Active and Assisted Living

Trust *vs*. control: the dilemma between data distribution and centralization

Alain Sandoz* - Léa Stiefel
University of Neuchâtel, Switzerland – University of Lausanne, Switzerland
alain.sandoz@unine.ch – lea.stiefel@unil.ch

Extended abstract

This paper reports on the motives, design, and implementation of a permissioned peer-to-peer platform for the authorized transmission of sensitive data between organizations of an economic sector, agriculture in Switzerland. The period under consideration spanned five years between 2015 and 2019.

Context of emergence

The peer-to-peer platform emerged indirectly because of an apparent need for greater efficiency in data management. After years of digitization of agricultural policies and of market adaptations, farmers were said to be burdened with data-related administrative tasks (Droz, 2014). They were supplying information to numerous organizations, both public and private, which in return provided subsidies, premiums, or other services related to the farm's needs or production modes. Each organization digitized and recorded sensitive information in its database, with redundancies and inconsistencies among these independent systems. Farmers' data was nevertheless controlled for accuracy by some organizations, which carried the risk of penalties, and farmers were under increasing pressure to make this sprawling system work. In 2015, a group of private actors floated the idea that efficiency would be improved if *all of the sector's data* were centralized *in one unique database* (that the same group would operate). Other parties, such as public administrations or producers' organizations, would be allowed to interoperate with the central database using application programming interfaces

(APIs). For reasons that are documented elsewhere, the proposal prompted a wave of protest and led to the launch of a counter-project for an alternate approach to data management (Stiefel, 2022). The project developed a peer-to-peer platform for organizations and farmers to solve the dilemma between data distribution and centralization, which is the subject of this paper.

The present work is the result of a collaboration between the platform's architect (a computer scientist) who led the project and was its chief strategist, and the ethnographer (a social scientist from the STS field) who followed its developments. The first author worked for a consortium of professional organizations that represented over 50% of Swiss farmers. The second author went behind the scenes of the project and in parallel conducted interviews with organizations and farmers to explore concerns related to the issues of data and data sharing.

Data

Switzerland is a small landlocked country in Western Europe. Apart from marginal forestry and fishery activities, agriculture is the only primary sector in the country, with some 53'000 farms, generally small family businesses. Many other actors make up the value chain uphill and downhill of production itself, and numerous organizations, public, para-public or private, structure the sector, from the import of machinery and fertilizers, down to the processing and distribution of food staples, flanked by professional defense, production control, and regulation. All these actors use digital systems and data to support their activities.

Farmers use digital systems in *production* and for *management*. Systems are developed by the agroindustry and/or software providers. On-farm systems use data to deliver functionality. Sources of data can be machines, sensors, or robots, or remote systems *e.g.*, weather stations. The farmer him/herself supplies data, *e.g.*, dates and places of sowing, types of crop or animal treatment, or quantities of produce and income, or costs, etc., used for resource planning. Data for production or management is often stored remotely, in databases operated by independent (and competing) service providers. These systems also compute, produce, and accumulate data. Production data can be sensitive for the service provider, because it is used to improve the system and has indirect market value. It is also sensitive for the farmer, as it describes modes of production that can be contracted or strictly regulated. Management data is sensitive because it is related to quality and quantity of production, as well as to financial, legal, or fiscal aspects, which, if disclosed, could jeopardize the farmer's position relatively to commercial partners, public regulators, and/or their respective control organizations. The evolution of digital technology *as a service* has brought advantages to farmers as it sometimes simplifies management, and enhances the quality and availability of information. It has also largely benefited database operators by giving them free and unrestrained access to huge amounts of valuable data.

Another type of digital systems that use data from farms are information systems of organizations that interact with farmers both collectively and individually: public administrations supervise the implementation of legislation, notably for subsidies, statistics, and policy-making; producers' organizations define requirements for labels (*e.g.*, organic, integrated, traditional, etc.) and quotas, which, if respected by the farmer, bring a premium on the market; professional organizations compute statistics to define their policies and political lobbying strategies; etc. All of these organizations need data from the farmers who are compelled to supply the data if they want to have a shot at the promised benefit. This data is even more sensitive than the production & management type, because on one side, it is specific to individual farms, but on the other it is collective, homogeneous, and often has a wider coverage than service providers can collect from their market share. Database operators (private or public) will have a precise view of a question, both general and specific to each farm.

To summarize: digital representations of sensitive information on farms are maintained in dispersed databases operated by independent service providers and organizations in the sector (data users). And farmers (data owners) want -in fact, need- to keep control of which actors have access to what data. On the other hand, their livelihood requires from farmers to supply large amounts of data to many organizations, including data that is not sensitive (or that can even be public, such as addresses), that is useful in different ways to different actors, and that is partially redundant and sometimes inconsistent.

Over time, managing the data that a farmer supplies to his/her numerous different "partners" became a problem of its own, and a burden. The problem was more often seen by farmers as the uncontrolled gluttony for their data of all sorts of benevolent organizations. But "data-sharing" between organizations[1] then suddenly popped up as the "solution" to the farmer's problem. The prospect of seeing some powerful actor forging the ability to compare data from his/her farm, compiled from different sources and providing answers to different questions, with all the other farms, became a farmer's digital nightmare.

Designed as a counter-measure to that yet unchecked perspective, authorized transmission between organizations *vs.* centralization by one privileged operator was a radically different approach to the problem of data management in the sector.

How farmers and organizations actually perceived the situation

This article is the result of a multidisciplinary collaboration between its two authors. In January 2018, the PhD student had just started her thesis and was interested in tracking the dynamics of digitization in the Swiss agricultural sector. She had attended a public presentation of the peer-to-peer platform by the architect

[1] A notion that goes well beyond the simplistic view of interoperating databases (Hummel, *et al.*, 2018).

and introduced herself, asking him to ethnographically follow its developments. At their second meeting in May 2018, the terms of their collaboration were set.

The ethnographer would be able to go behind the scenes of the project, and to follow and document all its developments. In return for full access, she would provide the architect with regular feedback on her observations, according to the rules of her discipline and her progressive understanding of digitization, via anonymized reports of her interviews. In addition to the practice of his own discipline and professional experience, the architect would benefit from this informed perspective to drive the project within its socio-technical environment.

The ethnographer conducted her interviews between January 2018 and September 2019 with some 40 actors in the Swiss agricultural sector, farmers (5), but especially representatives of agricultural organizations: agents of public administration (11) and professional defense (2), representatives of control bodies (6), certification bodies (2), professional associations and companies in the animal and dairy sectors (6), IT service providers for agriculture (4), and system operators of these same organizations (7) (in parallel, the architect held project and information meetings with over 50 representatives of public and private organizations, farmers and researchers, covering in particular the Eastern part of Switzerland[2], which he also reported back to the ethnographer).

Her interviews documented a range of concerns and risks perceived by farmers (data-owners) and agricultural organizations (data users) regarding the data centralization project that proposed to collect all data in a single database and, on this basis, to develop smart-farming services (decision support modules). Among its shareholders were the largest agricultural cooperative in Switzerland, both the farmers' main supplier and a major buyer of their products, a European software development company, linked to the cooperative by a German machinery manufacturer, and two important publicly owned, resp. supported, organizations.

For data-owners, the fact that the project was backed by such a conglomerate of powerful private players was a source of concern. The centralized database promised to provide its shareholders with full visibility into what was happening on all farms, and on a daily basis. Combined with its decision-support tools, the database would allow them - the cooperative and its foreign partners - to drive the demand for inputs and the supply of agricultural products, and to influence market and supply prices. The risk of "vertical integration" was great for farmers, who would meanwhile retain the burdens of dept and production risks (such as losses due to weather or disease). Moreover, they would have to pay for access to "services" developed on the basis of *their* data, the quality of which they would be held *liable* by contract, while all the profits would go to the database owners.

In addition, it was unclear how data would flow between partners associated with the centralized database. Without control over the flow of their data, farmers

---

[2] German-speaking, in contrast with the French-speaking Western part (origin of both authors) and with the Italian-speaking Southern part (marginally covered, with approx. 4% of the Swiss population and 2% of farms).

were at risk. If data inadvertently reached a government agency, indicating high nitrogen levels in one field that were compensated in another (which can happen every day on any farm), the farmer could lose subsidies. If data from a government inspection showing a health problem in an animal was inadvertently passed on to a dealer, the farmer, and even neighbors, could be sidelined for fear that disease might spread from the shipment to the slaughterhouse (what actually did happen to an entire village because of a single sick animal).

Finally, the push for smart-farming was problematic for farmers, who saw it primarily as a debt driver. Smart-farming was expensive and of little interest for Switzerland because of its lack of applicability in its mountainous, small scale and tradition-oriented agricultural model. Smart-farming favored industrial methods for export crops and intensive livestock that were incompatible with the quality-driven, environmental, and legal frameworks of Swiss farming.

For data-users, *i.e.*, the Swiss agricultural sector organizations, centralization also posed problems. If farmers were to enter their data into a single database, the organizations would have to "log in" to the database to access the data they needed (previously supplied directly by farmers). Farmers' data is of great importance to the organizations. Public administrations provide subsidies to farmers, compile statistics for the evaluation and development of agricultural policy, and control epizootics on the basis of data provided by farmers. Private organizations base their services on farmers' data, some of which are supported by the regulator, such as improving the genetic profile of animal breeds to ensure their resistance to pathogens. But there were no guarantees that they would actually be allowed to access the data in the centralized database, in contents and formats, and at times necessary to carry out their duties, nor was there any indication of the price to be paid. Centralization promised to jeopardize the autonomous management of the organizations' activities, to the point of threatening their very existence.

The project also foresaw to store all farmers' data in a cloud in Germany, under the control of the European software company partner. This posed a problem of data sovereignty, which was unacceptable to public administrations. It also posed problems as to how to resolve conflicts between farmers and organizations arising from data management, with data residing in the legal realm of a foreign authority.

The promoters promised that organizations could propose functional modules connected to the central database. But it was not clear to these organizations if this openness would be observed in reality beyond the rhetoric. The shareholders could very well act single-handedly, as long as they controlled the APIs. More fundamentally, this single, centralized database would introduce a distortion of competition. Faced with powerful foreign shareholders, who would concentrate all the farmers' data, smaller Swiss organizations wouldn't stand a chance to compete, which would sound their death knell.

Finally, private actors (device and machine manufacturers, service and software providers, etc.) who were not in the consortium and not part of the discussion simply waited for the storm to pass.

How the peer-to-peer platform worked

In Switzerland, each organization is legally and technically independent, and is liable towards the owners of sensitive data it manages on the base of some contract (explicit, or implicit as in the case of public administrations representing the regulator). In particular, data can be accessed online by a farmer only if the latter has been identified and authenticated by the database operator.

If data owned by a farmer were to be *transmitted* from one database to another, this would have to be with that farmer's authorization. Authorizations could be set and revoked at any time (by farmers using a mobile application) and were specific to *i*) one farmer, *ii*) one pair (sender-receiver) of database operators, and *iii*) one *datatype*. As long as an authorization was valid, the (willing) sender could send the famer's data of that type to the (requesting) receiver (using a three-step asynchronous protocol). Authorizations and transmissions were traced so that they could be recovered in case of suspected misconduct (a process that would be supervised by an auditing authority or a judge). Each peer (data user) operated its IT infrastructure under its own legal responsibility, including the platform's component, called *node*, that was its access-point to other peers, and the place where its transmissions were traced. For each sender-receiver pair, the datatypes that could be transmitted, for what purpose and under what conditions, were published on the platform by the operators. How authorizations were managed and how transmission was implemented in each node was transparent and certified (the platform was an open standard). However, what data was actually transmitted, with what values and when, was known only to the three parties involved: the owner, the sender, and the receiver, and transmission was direct between the latter two.

Design rationale and constraints

As mentioned above, the identity of the owner must be determined whenever the data is required for an operation, and access to the data by programs must be controlled. The organizations that operate the database and application servers that run the programs to provide a service to the owner are *de facto* users of the data. These systems are specific to each application domain (cereals, livestock, milk, etc.), and often to the organization itself. They have evolved over long periods of time and are heteroclite and heterogeneous assemblages of technologies. Low-level interactions between the legacy components and the solution would be specific. To simply distribute a software package that would be installed within their legacy infrastructure to implement authorized data transmission between organizations was not a technical option. The solution also needed to be isolated from that

infrastructure, so that a peer could disconnect from the platform without any other loss of functionality other than data transmission to others. A detailed description of how this was envisioned *in general* was fundamental to making an infrastructure acceptable to its future users (be they data owners or data users). This was provided by choosing the standard components (middleware, interface framework, and general-purpose functions) of the platform from free open-source, widely respected, software projects.

However, it was hardly enough to convince operators to adopt the system, and less even, to *share* their data with other organizations. A set of *principles* was established and communicated to the organizations, and then strictly implemented by the project (without any compromise or trade-off, for any reason). This covered the part of the development specific to authorized data-transmission. It was also to be freely distributed as open-source. The platform was *fully* distributed: it had no central component and all roles were completely *symmetrical* (what a peer could, every peer could, with the same constraints). Distribution of the platform ensured freedom of association, equal treatment, and symmetry among peers (Stiefel, Sandoz, 2022). Being neutral with respect to power relations between peers, the platform could enhance trust between operators. *Functionally*, the design was limited to the transmission of data between users (in the above sense), when and only when the data owner authorized it. Data was sent and received, and stored and accessed, only by the peers that used the given data, under separate and mutually unknown contractual conditions they had established with the data owner. Transmission, if authorized, was bilateral and direct between peers. Traces required for a peer to positively prove *correct* behaviour were always left locally and under the control of that peer only. Control data could not be forged (without the collusion of a qualified majority of peers). It could only be removed from a node by its peer, because of the latter's full local control. Consequently, there could be no proof of *misconduct*, only an absence of proof of correct behaviour, that could then lead to the suspicion of a rule violation. These considerations follow the technical line of what is possible or not in a distributed system under the principles stated above. It is not the purpose of this extended abstract to go into the details (nor *e.g.*, to argue why data transmission *was not* realized using blockchain technology[3]), but only to mention that the system design was keen on meeting its principles.

However, this still did not seem sufficient: legal requirements (collective contracts, node certification, general public licensing of the platform) were added to bring operators to adopt a model of action acceptable to the community of farmers (and among the organizations themselves).

---

[3] In particular, blockchain technology orders state changes using a decentralized computation that can delay certain operations in order to achieve consensus, thus potentially threatening participants' control over local operations; whereas in our case, neither consensus, nor ordering among all peers, was required globally to establish a farmer's authorization and to achieve bilateral data transmission among the peers involved. Only the full control of all three participants over any part of these operations was necessary.

Technically, the project faced two problems: 1) *asynchrony* in distributed systems (which is usually overcome by using the master-slave paradigm underlying internet protocols based on APIs); and 2) *matching the different meanings attributed to information* by a sender, a receiver, and a farmer *using digital data* (which is usually overcome by imposing data standards and formats between operators, without asking the data owner's opinion). The first problem was solved based on the properties of communication in distributed systems, which were established at the time of the architect's PhD thesis, early in the 1990s. The latter was trickier because, on one side, farmers (as well as most employees in organizations) are not familiar with the concept of digital data, and, on the other, most IT technicians have no idea of the gap between digital data and the information it is meant to represent. A mechanism called *segmentation* was designed and implemented in the project, and used to bridge the gaps in time and meaning that existed between organizations that would exchange data over the platform. The same mechanism underlay the touch-screen graphical management-app for authorizations used by the farmer. Since organizations would know how to link information they managed for farmers to digital data by using segmentation, it was foreseen that the partners that farmers trusted (*i.e.*, the professional organizations *from* which they were willing to have their data *sent* to others) would help them manage their authorizations by providing guidelines and templates.

The technologies and technical mechanisms used to implement a platform with these characteristics must either be broadly available or represent a small set of specific features that will be made freely available (Sandoz, 2020). To integrate the platform, operators' legacy production infrastructures could not be modified, but only *extended* in cheap and standardized, yet secure, ways, without affecting the mission or function of these systems. The platform architecture, node implementation, and connection of legacy systems to nodes, were based on the Kubernetes (K8s) microservice architecture, respectively the gRPC interface framework and the Hyperledger Fabric distributed ledger. The latter two technologies were available at the time of the project on top of K8s and all three were freely available in OS code. Mastering these technologies was at that time a big effort for any IT operation, especially those of organizations active in agriculture. Connecting a legacy system to its node through gRPC could also be challenging, depending on the legacy system. The project proposed to *lease* certified nodes to organizations as long as would be required, and to help them connect their legacy infrastructure to their node. The collective effort invested in the platform would bring the investment by individual organizations to build and configure their node down to a couple of man-months. At least one operator (operating the public database of five cantons) proceeded to migrate *completely* to K8s *during* the course of the project and was still happy with the move in March 2021. The platform and its technical architecture were also openly described as a modern initiative by an operator who managed the databases of four other cantons.

With this approach, the cost of the platform for any peer was very low, compared to what would have been required to build and maintain APIs to an alternate central database for all agricultural data. And additionally, the risks remained under each organization's control.

Conclusions

The platform was designed to address the concerns of data owners and of data users, and to support mutual trust with its socio-technical architecture (Mazzella, 2016). Farmers demand privacy from the organizations that manage their data. They trust them more or less willingly to provide services in accordance with the information they supply about their farms. They don't necessarily trust those organizations to use their data properly, transparently, and solely for their customers' benefit. An architecture that relies on transparency in how data is collected and used by operators could enhance trust. In a framework with clearly defined rules, control mechanisms and sanctions, and that the user community itself can steer according to changing conditions and needs, possibly under the guidance of external authorities (Hess and Ostrom, 2007), farmers might better accept, and push for, data sharing. Data management might then become more efficient.

The peer-to-peer platform was designed and developed with this in mind. Initiated in early 2018, it went into production in mid-2019 as a first productive prototype with five peer-demonstrators.

References

Droz, Y., Miéville-Ott, V., Jacques-Jouvenot, D., and Lafleur, G. (2014): *Malaise en agriculture. Une approche interdisciplinaire des politiques agricoles France-Québec-Suisse*. Karthala Editions, Paris.

Hess, C., and Ostrom, E. (eds.). (2007): *Understanding Knowledge as a Commons. From Theory to Practice.* The MIT Press, London.

Hummel, P., Braun, M., Augsberg, S., and Dabrock, P. (2018): "Sovereignty and data sharing", ITU Journal: *ICT Discoveries*, Special Issue No. 2, 23 Nov. 2018

Mazzella, F., Sundararajan, A., D'Espous, V., and Möhlmann, M. (2016): "How digital trust powers the sharing economy". *IESE Insight*. Vol. 30. No. 3. 10.15581/002.ART-2887.

Sandoz, A. (2020): *Inter-operating Co-opeting Entities: A Peer-to-Peer Approach to Cooperation between Competitors*. Proceedings of the 10th Int. Conf. on Business Intelligence and Technology. Nice, Oct. 2020.

Stiefel, L. (2022): "Les données du problème. Une plateforme numérique inadaptée à l'agriculture suisse". *Etudes Rurales*, No. 209 / 2022. Editions de l'EHESS. *In press*.

Stiefel, L., and Sandoz, A. (2022): *Critique de la concentration: une analyse des relations de dépendance sur les plateformes numériques*. Proceedings of the XXXIst AIMS Conf. on Strategic Management. Annecy. 31 May – 3 June 2022. *In print*.

Carina Dantas, Karolina Mackiewicz (2022): Are we ensuring a citizen empowerment approach for health data sharing? In: Proceedings of the International Conference on Privacy-friendly and Trustworthy Technology for Society – COST Action CA19121 - Network on Privacy-Aware Audio- and Video-Based Applications for Active and Assisted Living

Are we ensuring a citizen empowerment approach for health data sharing?

Carina Dantas[1,2], Karolina Mackiewicz[1]
[1] European Connected Health Alliance, [2] SHINE 2Europe
carina@echalliance.com, carinadantas@shine2.eu; karolina@echalliance.com

Abstract

Today, almost all (if not all) societal activities, especially in the health field, involve the collection and processing of large amounts of data. Technological advancement, with an emphasis on the exponential increase of eHealth apps, implies that the data collected in this field will quickly become very extensive, up-to-date and timely. However, some major ethical and technical challenges arise when using big data to support health predictions, such as data protection and privacy, safe storage and analysis, scalability, potential security breaches and the capability to protect citizens rights, among others.

These concerns are already widely perceived by the European policy makers and are being addressed in communications, regulations and initiatives of several Member States, as well as EU projects, such as CA19121 – GoodBrother [1].

Being a fairly new area with many open questions, data sharing is a subject that is far from being discussed by the common citizen and a clear elicitation of its potential benefits will be key to active engagement. Besides an increase in trust, clear explanations on how and what data is collected, namely in video and audio-

based applications, how can data sharing work in practice, what direct benefits can be achieved by the individual and by society and what are the low hanging fruits that can be collected are essential for the involvement of citizens in the data sharing movement.

Background

Europe has already passed the point where healthcare and social care systems are able to respond to all upcoming needs and inequalities related to access to healthcare in a traditional way. Thus, these issues need to be addressed through a coordinated approach that builds on the use of new technologies and health data for diagnosis, treatment and care. The outbreak of COVID-19 made the need for health and health-related data much more visible [2] and raised discussions about data sharing schemes, citizens' control over their data and potential data governance models, mainly due to the tension between public health interest vs citizens privacy and security of data [3], [4].

To guarantee sustainability of the healthcare systems it is necessary to invest in prevention and predict the upcoming challenges with enough time to address them with the minimum resources [5]. This is in line with the United Nations Sustainable Development Goals [6], as well as the whole-of-society and whole-of-government approaches. However, this raises additional challenges such as the eSkills of healthcare professionals, digital health literacy of the population and the need for capacity building of local, regional and national authorities.

Research must invest in predictive analytics - determining the biggest at-risk factors by analysing the factors taken from different sources over the course of people's lives, thus preventing health problems from developing. This predictive research is now quite fallible due to the small samples of data available that are used to extrapolate results. Big data is often discussed in the context of improving medical care, but it could have an even more relevant role in preventing disease, by increasing the effectiveness of interventions to help people achieve healthier behaviours in healthier environments [7].

However, some very relevant challenges arise when using big data to support health predictions. Especially, when considering audio and video-based Ambient Assisted Living (AAL) products and services, ethical and technical concerns are extensive and require improved methods and larger discussion [8, 9].

Data protection and privacy still entail further developments and high investment in order to positively impact trust and citizen reliability on digital

services and tools. Data protection becomes more challenging to ensure as information is multiplied and shared around the world through multiple technological devices. Information regarding individual's health, location, online activity, among so many others, raises reasonable concerns about profiling, discrimination, exclusion and loss of control.

Also, safe storage and analysis, scalability, potential security breaches, the capability to protect citizens rights, prevent cyberattacks and misuse, are all very important issues that still need further developments.

These concerns are already widely perceived by the European policy makers and are being addressed in communications, regulations and initiatives of several Member States [10, 11].

A practical example of how to address these societal and ethical challenges in the development of video or audio-based AAL services is the use of ethical dialogue iterations with the relevant stakeholders, leading to an interactive process of co-creation throughout the development and deployment of the product [12]. The ethical dialogue starts with a contextual explanation of how the product or service work, (e.g. surveillance by sensors, cameras, storage of personal information etc.), followed by an open discussion on the perspectives of the participants involved regarding the effects of the technology, the specific aspects of implementation and what should be changed, adapted or improved based on stakeholders' feedback. The participation of the quadruple-helix of stakeholders in this dialogue process includes end-users, caregivers, health professionals, payers, policy makers and any others that may be relevant to the product or service at stake. Most user engagement methods foresee involving only the end user, but not the whole range of stakeholders that are somehow of relevance. However, the whole value-chain is essential to ensure that products and services are answering user needs and also adjusted to professionals demands, reimbursement models and fit to the different national markets This interactive and iterative discussion between different actors brings several more challenges (and potential solutions) to the table, thus enriching the potential results and market feasibility for the future.

This method is already being used by the AAL Association in a batch of pilots within their approved projects for funding for the last two years and the assessment is so far very positive.

Towards a citizen empowerment approach

Besides the support and boost of European industry competitiveness, it is a priority for Europe that citizens and patients have the right to and should be empowered to determine when and how their health data can be shared, by having secure and authorised access to it and being able to securely provide these to authorised parties. By enabling this, it becomes possible to reengineer today's practices on citizen consent in a fully informed way and specific to the context of sharing, even in the most challenging situations such as for re-using data for research purposes.

For example, the Data Governance Act [11] brings forward the concept of Data Altruism as "data that is made available without reward for purely non-commercial usage that benefits communities or society at large, such as the use of mobility data to improve local transport" which underlies a strong and beneficial societal purpose. However, when being implemented, it should not be a legal expedient to justify accessing all data sources potentially needed for research, without the need for citizen consent. This would again break the trust chain with the citizens. For purposeful and large-scale data sharing Europe needs an educational pathway that is long-term and implies a cultural shift and an empowerment perspective in terms of literacy, citizenship and democratic participation. Even if shorter-term solutions are needed to enable data sharing, data altruism should be a holistic and beautiful vision of a committed society and not only a legal opportunity or an ethical obligation to share data.

For citizens' and patients' full empowerment however, it is important to rethink the way health data is captured, stored and organized, especially when concerning video and audio-based AAL tools. It needs to become easily discoverable, consistent across several health information providers and over time, shared across communities securely and lawfully through systems and apps that support interoperability.

But mostly, it also needs to ensure users that their intimacy and private life are not disclosed. There is the fear that some data platforms, especially those marketed directly to citizens, may poorly protect against cyber security risks as well as risks of privacy breaches, due to lack of supervision. To overcome these barriers, efforts must be strengthened and escalated in all areas of interoperability, data quality, clinical and co-operative governance.

In this context of citizen-controlled data governance, it is essential to further understand and experiment with digital empowerment models that are in use in

Europe and beyond, framed to examine innovative and ground-breaking initiatives that may be benchmarked and adopted to overcome the challenges.

Being a fresh new area, data sharing is indeed a subject that is far from being discussed and comprehended by the common citizen. However, this knowledge, understanding of the process and a clear elicitation of the potential benefits connected to data sharing will be key to active engagement and the use of digital applications for health.

Side by side with the need for more trust in the process, public campaigns and clear explanations of how data sharing can work, what direct benefits can be achieved by the individual and by society and what are the low hanging fruits that can be collected – e.g., privileged access to research results – will be essential for the involvement of citizens in the data sharing movement, as future works to be developed.

Acknowledgments

This work was partially developed within the DigitalHealthEurope project, funded by the European Commission under the Grant Agreement: 826353 (https://digitalhealtheurope.eu/) and based upon work from COST Action GoodBrother 19121 – Network on Privacy-Aware Audio- and Video-Based Applications for Active and Assisted Living, supported by COST (European Cooperation in Science and Technology).

References

[1] COST action 19121, Network on Privacy-Aware Audio- and Video-Based Applications for Active and Assisted Living. Accessed: March 18th, 2022. Available: https://goodbrother.eu/

[2] WHO on behalf of European Observatory on Health Systems and Policies, "Quarterly EUROHEALTH", 2020. [Online]. Accessed: March 18th, 2022. Available: https://apps.who.int/iris/bitstream/handle/10665/336263/Eurohealth-26-2-2020-eng.pdf

[3] Organisation for Economic Co-operation and Development, "Recommendation of the Council on Health Data Governance, OECD/LEGAL/0433", 2019. [Online]. Accessed: March 18th, 2022. Available: https://www.oecd.org/health/health-systems/Recommendation-of-OECD-Council-on-Health-Data-Governance-Booklet.pdf

[4] World Health Organization, "Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing. Interim guidance", 2020. [Online]. Accessed: March 18th, 2022. Available: https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1

[5] C. Dantas, W. van Staalduinen, M. van der Mark, A. L. Jegundo, J. Ganzarain. “Framing Paper Thematic Network 2018 Smart Healthy Age-Friendly Environments”. https://en.caritascoimbra.pt/wp-content/uploads/sites/3/2018/11/Framing-Paper-SHAFE-20181121.pdf

[6] United Nations. “Take actions for the sustainable development goals”. Sustainable development goals. https://www.un.org/sustainabledevelopment/sustainable-development-goals/

[7] M. A. Barrett, O. Humblet, R. A. Hiatt, and N. E. Adler, “Big Data and Disease Prevention: From Quantified Self to Quantified Communities,“ Big Data, vol. 1, no 3, pp. 168-175, Sep. 2013, doi: http://doi.org/10.1089/big.2013.0027

[8] E. Vayena, T. Haeusermann, A. Adjekum, and A. Blasimme, “Digital health: meeting the ethical and policy challenges”, Swiss medical weekly, 2018, doi: 10.4414/smw.2018.14571

[9] UNGlobalPulse, “Data privacy, ethics and protection: guidance note on big data for achievement of the 2030 agenda” 2017. [Online]. Accessed: March 18th, 2022. Available: https://unsdg.un.org/sites/default/files/UNDG_BigData_final_web.pdf European Commission, “A European strategy for data”. Shaping Europe’s digital future. [Online]. Accessed: March 18th, 2022. Available: https://digital-strategy.ec.europa.eu/en/policies/strategy-data

[10] Dantas, C., Hoogendoorn, P., Kryspin-Exner, I., Stuckelberger, A. & Tijink, D. “AAL Guidelines for Ethics, Data Privacy and Security”, 2020. Ambient Assisted Living Association. Available: http://www.aal-europe.eu/wp-content/uploads/2020/07/AAL-guideliens-for-ethics-final.pdf

[11] European Commission, “Proposal for a regulation of the European parliament and of the council on harmonised rules on fair access to and use of data (Data Act)”, 2022. [Online]. Accessed: March 18th, 2022. Available: https://digital-strategy.ec.europa.eu/en/library/data-act-proposal-regulation-harmonised-rules-fair-access-and-use-data

[12] A. M. Vicente, W. Ballensiefen, D. Donertas, M. Eklund, A. Ivask, J. Jönson, K. Kulmann, A. Lawrence, M. O’Driscoll, E. Richer, and G. Trivella, “The ICPerMed vision for 2030. How can personalised approaches pave the way to Next-Generation Medicine?”. ICPerMed International Consortium, Sep 2019. [Online]. Accessed: March 18th, 2022. Available: https://www.icpermed.eu/media/content/Vision_Paper_2019.pdf

Anton Fedosov, Liudmila Zavolokina, Sina Krumhard, and Elaine Huang (2022): Toward unpacking trust in a local sharing economy community. In: Proceedings of the International Conference on Privacy-friendly and Trustworthy Technology for Society – COST Action CA19121 - Network on Privacy-Aware Audio- and Video-Based Applications for Active and Assisted Living

Toward unpacking trust in a local sharing economy community in Switzerland

Anton Fedosov, Liudmila Zavolokina, Sina Krumhard, Elaine Huang
University of Zurich, Switzerland
antonf@ifi.uzh.ch, zavolokina@ifi.uzh.ch, sina.krumhard@uzh.ch, huang@ifi.uzh.ch

Background

The rapid development of the social, economic, and business models of the "sharing economy" [2] enables the effective and efficient coordination, acquisition, distribution, and sharing of many kinds of different resources. Beyond well-known services such as Airbnb and Uber, an increasing number of sharing initiatives have established online platforms and services to facilitate access to shared resources (e.g., tools, food surplus, spaces) within their local communities. With the automation and complexity of digital tools and platforms, and the specific challenges of online sharing communities [6], trust within supporting technologies become increasingly critical for successful use and adoption [4,13].

Trust is the basis for many human interactions and relationships. Furthermore, the concept can be transferred to institutions, organizations, and technologies [1,3]. Today, trust in technologies is especially important as it is a prerequisite for successful technology adoption [8,11]. The importance of trust in technologies has been examined by scholars in different settings such as virtual communities [16],

e-commerce systems [9,18], online exchange communities [12], and other contemporary digital services and platforms that facilitate economic interactions among peers [3]. Interactive systems can have two different roles in trust relationships [18]. The first is the mediator role, in which a system mediates an interaction between humans. For this role, interpersonal trust should be established. The second is the trustee role, in which a system is the agency a human interacts with and, thus, needs to be trusted. For this role, systems trust should be established.

In most cases, today's digital solutions are 'black boxes' [17] for users. Explaining how a digital solution is developed and how its algorithms function does not necessarily lead to more trust [17]. Therefore, new approaches are needed to engender trust and to design trustworthy digital solutions in which algorithms play a more active role than before. For example, *trust-supporting design elements* [15,21], which are platform features that establish end-user trust, can help establish trust in 'faceless' algorithms.

In online sharing communities, designers of platforms have the challenge of designing for both interpersonal and systems trust to ensure effective and meaningful interactions among their users [10,19]. With the advent of rapid digitalization, the emergence of new digital solutions, and the pressure to stay competitive, service providers further develop online platforms and introduce new features and mechanisms, which may distort previously established trust in systems.

In our empirical study, we aim to unpack elements of interpersonal and systems trust in the case of a local online sharing community which recently introduced a new semi-automated mechanism for resource exchange.

Case Study

We are conducting a study in collaboration with two companies in Switzerland: a Zurich-based two-sided online marketplace [12] for household goods, Sharely[1], and the Swiss Federal Railways (SBB). Sharely aims to increase sharing and use of underutilized personal items (e.g., a drill, a bike pump, sports equipment), by advocating conscientious and sustainable resource consumptions practices (e.g., "better to share than to buy"). Community members can post information about the items they want to lend on Sharely's website or mobile app. These items can be borrowed for a small fee from a lender for a fixed period of time. Sharely takes a percentage of each transaction on their platform. The pick-up and return of the items are decided by the lender and borrower and usually happen face-to-face.

Recently, Sharely added a new service that offers members an option for indirect resource exchange (e.g., [14]), i.e., where pick-up and return do not happen through face-to-face interaction. In a partnership with SBB, Sharely enables renting

[1] https://www.sharely.ch/

popularly exchanged items using SBB SMART BOXES[2], newly repurposed luggage lockers at train stations. The SMART BOXES are Internet-enabled lockers that can be opened and closed via a mobile app. In this context, Sharely provides a small set of its most popular items (e.g., a drill, a jigsaw, a drone), which users can borrow via the SMART BOXES in a semi-automated manner in one pilot site station in Zurich.

The new sharing system introduced by Sharely and SBB faces some trust-related challenges in both interpersonal and systems trust [4]. Therefore, we formulated two research questions for our study:

(1) What are the current conceptualizations of interpersonal and systems trust in the Sharely community?
(2) How can they be shaped by the introduction of an impersonal exchange through the SBB SMART BOX?

Prior research indicates that face-to-face exchanges are critical for establishing trust in local resource-sharing communities [7]. In this new setting, interpersonal trust within the community could be hard to maintain. In the case of broad deployment of this new exchange option and its integration into peer-to-peer sharing arrangements, both the lender and the borrower miss out on the opportunity to meet face-to-face as the trust is placed in a system rather than in other members [12].

When it comes to systems trust, successfully mediating trust from Sharely's website and service in this new sharing arrangement may pose another challenge to trust accrual and maintenance in the community and their supporting technologies. More specifically, it is unknown how the introduction of indirect resource exchange shapes members' perceptions of usability and reliability of the Sharely and how it affects peoples' attitudes toward privacy and safety, which are constitutive properties of trust(worthiness) in computing systems [20].

Ultimately, we envision that studying the deployment and use of SMART BOXES could lead to insights into other developments in IoT automation in the sharing economy (e.g., the use of smart locks to grant access to shared apartments [5]). To date, the decision about renting out resources has generally been the prerogative of the resource owner, but we envision that in the near future, automated systems could take a more active part in helping communities identify and optimize available resources and easing the coordination of sharing through automated or semi-automated processes, bringing up a new set of characteristics to determine systems' trustworthiness, such as fairness, accountability, and transparency [20]. Subsequently, discussing the results of our empirical study about conceptualizing trust in a local online sharing community and identifying *trust-supporting design elements* for future (sharing economy) platforms motivate our interest in this conference.

---

[2] https://smartcitylabbasel.ch/en/projekte/sbb-smart-box/

References

[1] Balázs Bodó. 2021. Mediated trust: A theoretical framework to address the trustworthiness of technological trust mediators. *New Media & Society*, *23*(9), 2668-2690.

[2] Rachel Botsman and Roo Rogers. 2010. What's mine is yours. *The rise of collaborative consumption*.

[3] Rachel Botsman. 2017. *Who can you trust?: how technology brought us together–and why it could drive us apart*. Penguin UK.

[4] Coye Cheshire. 2011. Online trust, trustworthiness, or assurance? *Daedalus* 140, 4, 49–58.

[5] Rajib Dey, Sayma Sultana, Afsaneh Razi, and Pamela J. Wisniewski. 2020. Exploring smart home device use by airbnb hosts. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–8.

[6] Anton Fedosov, Airi Lampinen, Tawanna R. Dillahunt, Ann Light, and Coye Cheshire. 2019. Cooperativism and Human-Computer Interaction. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, 1–4.

[7] Anton Fedosov, Airi Lampinen, William Odom, and Elaine M. Huang. 2021. A Dozen Stickers on a Mailbox: Physical Encounters and Digital Interactions in a Local Sharing Community. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW3, 1–23.

[8] David Gefen, Elena Karahanna, and Detmar W. Straub. 2003. Trust and TAM in online shopping: An integrated model. *MIS quarterly*, 51–90.

[9] David Gefen and Detmar W. Straub. 2004. Consumer trust in B2C e-Commerce and the importance of social presence: experiments in e-Products and e-Services. *Omega* 32, 6, 407–424.

[10] Florian Hawlitschek, Timm Teubner, and Christof Weinhardt. 2016. Trust in the sharing economy. *Die Unternehmung* 70, 1, 26–44.

[11] Axel Hoffmann, Holger Hoffmann, and Matthias Söllner. 2013. Fostering initial trust in applications–developing and evaluating requirement patterns for application websites. In *21st European Conference on Information Systems (ECIS),* Utrecht, The Netherlands.

[12] Airi Lampinen and Barry Brown. 2017. Market design for HCI: Successes and failures of peer-to-peer exchange platforms. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 4331–4343.

[13] Airi Lampinen, Vilma Lehtinen, Coye Cheshire, and Emmi Suhonen. 2013. Indebtedness and reciprocity in local online exchange. In *Proceedings of the 2013 conference on Computer supported cooperative work*, 661–672.

[14] Matthew V. Law, Mor Naaman, and Nicola Dell. 2018. ShareBox: Designing A Physical System to Support Resource Exchange in Local Communities. In *Proceedings of the 2018 Designing Interactive Systems Conference*, 1155–1167.

[15] Jan Marco Leimeister, Winfried Ebner, and Helmut Krcmar. 2005. Design, implementation, and evaluation of trust-supporting components in virtual communities for patients. *Journal of Management Information Systems* 21, 4, 101–131.

[16] Jan Marco Leimeister, Pascal Sidiras, and Helmut Krcmar. 2006. Exploring success factors of virtual communities: The perspectives of members and operators. *Journal of organizational computing and electronic commerce* 16, 3–4, 279–300.

[17] Wolter Pieters. 2011. Explanation and trust: what to tell the user in security and AI? *Ethics and information technology* 13, 1, 53–64.

[18] Matthias Söllner, Axel Hoffmann, Holger Hoffmann, Arno Wacker, and Jan Marco Leimeister. 2012. Understanding the formation of trust in IT artifacts. Association for Information Systems. In *Proceedings of the International Conference on Information Systems (ICIS'12)*, Orlando Florida, USA.

[19] Maarten Ter Huurne, Amber Ronteltap, Rense Corten, and Vincent Buskens. 2017. Antecedents of trust in the sharing economy: A systematic review. *Journal of Consumer Behaviour* 16, 6, 485–498.

[20] Jeannette M. Wing. 2021. Trustworthy AI. *Commun. ACM* 64, 10, 64–71.

[21] Liudmila Zavolokina, Noah Zani, and Gerhard Schwabe. 2020. Designing for Trust in Blockchain Platforms. *IEEE Transactions on Engineering Management*.

Renata Mekovec and Dijana Oreški (2022): Competencies for professionals in the fields of privacy and security. In: Proceedings of the International Conference on Privacy-friendly and Trustworthy Technology for Society – COST Action CA19121 - Network on Privacy-Aware Audio- and Video-Based Applications for Active and Assisted Living

Competencies for professionals in the fields of privacy and security

Renata Mekovec, Dijana Oreški
University of Zagreb, Faculty of organization and informatics
renata.mekovec@foi.unizg.hr, *dijana.oreski@foi.unizg.hr*

Abstract

According to a new ISACA report, the long-standing privacy skills gap is now posing a serious security risk, as a lack of training, poor app/service design, and failure to detect personal data are all contributing to an increase in data breaches (ISACA 2022). On the other hand, the cybersecurity skills shortage is a problem for both economic development and national security because it poses threats to the data, information technology systems, and networks that serve as the frontal bone of modern societies (De Zan and Di Franco 2019). This lack can be seen from two perspective: quantitative and qualitative. The quantitative issue is the insufficient supply of professionals to meet the job market's requirements, while the qualitative issue is the inadequacy of professional skills to meet the market's needs.

The demand for privacy professionals is expected to rise over the next year, with technical privacy roles growing faster than legal/compliance roles (ISACA 2022). There was a 30% year-over-year increase in available privacy roles in 2021 and 2020, with the trend expected to continue, if not accelerate, through 2022 and beyond (Haher et al. 2022). Furthermore, a gap between demand and trained talent is growing. The reasons for this shortfall are numerous and varied. At the formal educational level (university, college), the number of students pursuing privacy or/and cybersecurity as a qualification has steadily increased over the last decade

or so, but the number of graduates continues to fall far short of industry demand. It takes time to educate and train highly skilled professionals, as well as time to gain practical on-the-job experience. Meanwhile, investment in privacy and cybersecurity training has been severely hampered as budgets for non-profit and revenue-generating items have been cut or reduced (Naden 2021).

A single data protection officer or other function will be incapable of administering, supervising, and enforcing data protection requirements manually without the assistance of a team or at least one assistant. To address information system threats and vulnerabilities, these professionals must understand the entire business of the organization, have extensive knowledge of information technology, and specific expertise in information privacy and security. They are expected to recognize the importance of investing in security personnel in order to develop and protect their entire organization. Privacy and security are gradually merging, with mutual interests and responsibilities.

The benchmark survey (CISCO 2021) asked security professionals to identify their top three areas of responsibility. "Data privacy and governance" was chosen by these respondents the most frequently (32 percent), just ahead of "Assessing and managing risk" and "Analyzing and Responding to Threats." Data privacy has become a core competency for these teams, in addition to all of the usual security functions. Armstrong et al. (2018) propose that students (in the domain of security) should graduate with the following skills: 1) knowledge of and skills in identifying vulnerabilities and robustness of systems and applications; 2) conceptual familiarity with attack classes and attack stages; 3) knowledge of and skills in penetration testing principles and tools; and 4) knowledge of network traffic and network protocols. ACM provided guidelines for associate-degree cybersecurity programs that should encompass eight knowledge areas: data, software, component, connection, system, human, organizational and societal security (ACM and CCECC 2020). According to ENISA a certified higher education cybersecurity degree should include (De Zan and Di Franco 2019): (1) enough specific credits dedicated to cybersecurity courses and activities; (2) a structured curriculum, which may include a practical/training component or specific types of examinations and activities such as cybersecurity competitions; (3) a high-quality teaching faculty, which may include industry lecturers; (4) a broader multi-/interdisciplinary focus; and (5) outreach activities and programs. In order to address the cybersecurity skills shortage, the European Cybersecurity Skills Framework aims to create a common understanding of the roles, competencies, skills, and knowledge used by and for individuals, employers, and training providers across EU Member States (ENISA 2022). NIST Privacy Framework is proposing privacy practices that support privacy by design concepts and assist organizations in protecting the privacy of individuals (NIST 2020).

The e-Competence Framework (e-CF) - A Common European Framework for ICT Professionals in All Sectors is a standard for ICT professional competence that

defines the minimum requirements of competence in ICT workplace (16234-1 2016). e-CF introduces transferable skills that can be used across all ICT competences. Transfer skills are necessary in all ICT-related operations in the age of IoT, AI, and Industry 4.0. The fact that security and privacy are two of the seven stated transversal factors demonstrates the importance of these skills.

Qualifications play an important role in improving employability, mobility, and access to higher education (C 189/15 2017). The European Qualifications Framework (EQF) is a common European reference framework aimed at making qualifications easier to read and understand across countries and systems. The EQF's core are its eight reference levels, which are defined in terms of learning outcomes, namely knowledge, skills, and autonomy-responsibility. The EQF has been a driving force behind the creation of comprehensive national qualification frameworks based on learning outcomes. All countries that have accepted on to the EQF presume that such national frameworks are required to make their qualifications comparable across sectors and countries. 35 countries had formally linked ('referenced') their national qualification frameworks to the EQF by September 2021.

The Croatian Qualifications Framework - CROQF is building a harmonization mechanism supply and demand for work at the level of competencies, which is helping to modernize and reform the qualification system in the Republic of Croatia (NN 22/2013). There is currently no occupational standard in Croatia that addresses privacy and security competencies. According to CROQF methodology for developing occupational standards and sets of competencies (Ministarstvo rada i mirovinskog sustava obitelji i socijalne politike) we conducted structured interviews with 24 employees of leading IT companies in Croatia to define the occupational standards for information security and privacy architects. They were managers' and lower-level employees' representatives (operatives). Their task was to express which jobs are performed by the company's person in charge of information security and privacy. Then they had to figure out what knowledge and skills are needed to do the job. Each knowledge and skill were evaluated to determine whether it was required or optional, as well as the level of expertise required to complete the task.

As result proposition of occupational standard Information security and privacy architect is defined which encompass following key jobs (and competences):

- Planning of information security and privacy systems, as well as organizational, technical, spatial, financial and human resources for deployment and monitoring system,
- Planning and designing the organizational structure for the implementation of the information security and privacy system in the business system,
- Conducting analysis and assessment of the current situation in terms of information security and privacy requirements,

- Assessing potential risks based on the identification of information assets, the importance of data content, possible sources and forms of threats using modern risk calculation methodologies,
- Proposing ways to deal with identified threats and measures for risk reduction,
- Development of a business system work plan in crisis conditions as well as proposing system recovery measures,
- Conducting security and privacy vulnerability testing,
- Managing the roles and responsibilities of jobs and assigning or withdrawing authorizations for information resources use,
- Developing policies and procedures for the design, storage, use and access of information system backups as well as passwords usage policies and procedures,
- Implementing categorization of software and critical software, as well developing a protocol for dealing with categorized software support in incident situations,
- Periodic reporting to the Management Board on the overall security and privacy situation of business system,
- Management of software updates (on all user workstations) in order reduce vulnerability,
- Establishing procedures for exercising individual rights related to protection security and privacy,
- Assist in the description, presentation, and marketing of a product or service in accordance with security and privacy requirements,
- Communicating with customers, suppliers, associates and other stakeholders while developing information security and privacy systems as well as with the supervisory bodies within the business system and in the environment,
- Exchanging experiences with similar business entities and professional associations in the country and abroad in order to harmonize and implement measures,
- Collaboration on security and privacy improvement projects, as well as participation in the development, improvement or innovation of products or services to meet security and privacy requirements while adhering to good practice, legislation, codes of conduct,
- Defining indicators related to security and privacy on the basis of which organization checks and monitors the progress of quality assurance, particularly in the development and/or upgrading a product or service,
- Raising moral and material responsibility for omissions or non-compliance with prescribed measures in the information security and privacy.

In addition to defining the structure of an occupational standard for Information security and privacy architects, we highlight variables important for identifying key jobs in the study. The latent class clustering analysis (LCA) is employed to account for heterogeneity across different groups of experts. LCA is data mining method

used to identify mutually exclusive latent groups (clusters) of experts considered to be homogeneous based on their responses to indicator variables: (i) perceptions of the key jobs that a worker with an occupation for which an occupational standard is developed are performed and (ii) necessary level of expertise for the job to be performed. An aim of this analysis was to identify clusters of experts with regard to their perceptions. We have developed numerous cluster models to identify optimal number of groups. The results revealed the existence of two latent clusters for each group of the jobs (e.g. workplace preparation, occupational jobs related to the workplace...), with different profiles. Experts of the same level of: (i) duties in organization and (ii) insights into jobs requirements, have similar perceptions.

References

Armstrong, Miriam E., Keith S. Jones, Akbar Siami Namin, and David C. Newton. 2018. "What Vulnerability Assessment and Management Cybersecurity Professionals Think Their Future Colleagues Need to Know." 1082–1082. doi: 10.1145/3159450.3162250.

ISACA. 2022. "Privacy in Practice 2022."

Naden, Clare. 2021. "ISO - The Cybersecurity Skills Gap." Retrieved April 12, 2022 (https://www.iso.org/news/ref2655.html).

16234-1, EN. 2016. E-Competence Framework (e-CF) - A Common European Framework for ICT Professionals in All Sectors - Part 1: Framework.

ACM, and CCECC. 2020. Cybersecurity Curricular Guidance for Associate-Degree Programs.

C 189/15. 2017. Council Recommendation of 22 May 2017 on the European Qualifications Framework for Lifelong Learning and Repealing the Recommendation of the European Parliament and of the Council of 23 April 2008 on the Establishment of the European Qualifications Framework for Lifelong Learning.

CISCO. 2021. Cisco 2021 Data Privacy Benchmark Study - Forget by the Pandemic: The Age of Privacy.

ENISA. 2022. European Cybersecurity Skills Framework Draft v0.5 Work In Progress APRIL 2022.

Haher, Rachael, Jared Coseglia, Lauren Strait, Michelle Shanik, Marketing Manager, Jess Barre, Sarah Roberts, Sarah Brown, Amelia Channell, and Brittany Hall. 2022. Data Privacy Jobs Report 2022.

ISACA. 2022. Privacy in Practice 2022.

Ministarstvo rada i mirovinskog sustava obitelji i socijalne politike. 2021. Metodologija Za Izradu Standarda Zanimanja i Skupova Kompetencija.

NIST. 2020. NIST PRIVACY FRAMEWORK: A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT, VERSION 1.0.

NN 22/2013. 2013. The Croatian Qualifi Cations Framework Act.

De Zan, Tommaso, and Fabio Di Franco. 2019. ENISA: Cybersecurity Skills Development in the EU - The Certification of Cybersecurity Degrees and ENISa's Higher Education Database.

Özkula (2022): The visibility paradox: empowerment and vulnerability in inclusivity processes. In: Proceedings of the International Conference on Privacy-friendly and Trustworthy Technology for Society – COST Action CA19121 - Network on Privacy-Aware Audio- and Video-Based Applications for Active and Assisted Living

The visibility paradox: empowerment and vulnerability in inclusivity processes

Suay Melisa Özkula
Marie Sklodowska-Curie Research Fellow, University of Trento
suaymelisa.ozkula@unitn.it

Extended Abstract

In the wake of the global Covid-19 pandemic, individuals and organisations have been subject to a growing reliance on digital media technologies and solutions offered by these (Newlands et al., 2020). This has, above all, resulted in a proliferation of video-conferencing technologies such as Zoom, Google Meet, and Microsoft Teams. While these technologies have been able to mitigate some of the pandemic effects and therefore become "the new normal" in various sectors, their growing use has also been met with a range of privacy concerns (Newlands et al., 2020).

Nevertheless, this transition to smart working has opened up new pathways of inclusion as underprivileged individuals and communities have previously been excluded from attending or presenting at events due to travel embargos or funding constraints. In particular, international organisations working with marginalized social groups, such as the wide spectrum of United Nations (UN) bodies and agencies, have capitalised on these new opportunities for inclusion and collaboration. As such, this development should provide social benefits, as concerns have been raised around exacerbated inequalities for ethnic minorities

and the working class (Madianou, 2020). This includes the exclusion and even invisibility of the "data poor", above all citizens in Global South countries (Milan & Trere, 2019). These inclusivity practices should therefore mitigate some of these effects.

This paper uses the case study of a UN process, here labelled "The Forum" [due to preliminary anonymization] based on a visiting research fellowship in 2022. Although UN agencies and their networks have attracted considerable trust from its constituents (e.g. Gilbert & Behnam, 2013), the global pandemic has created a range of unpredicted scenarios in technology use, above all live and recorded video-conferencing tools. This case study illustrates some of the challenges that these new opportunities for inclusivity and visibility have incorporated (in the case study as well as across organisations).

Preliminary findings showed a growing complexity and uncertainty in giving visibility to marginalised, disadvantaged, or largely "invisible" communities, individuals, and initiatives across the globe due to new practices incorporated in response to the global pandemic. These practices included the automatic collection of participant metrics in registration processes, live streaming practices of partially unscripted materials, and the recording and making publicly available virtual sessions. While these opportunities were largely embraced by constituents due to the increased visibility and therefore "empowerment", based on preexisting trust relationships, they also gave way to gaps in regulation and consequently concerns around what data may be collected as well as how it may be used. Questions were raised, for example, in cases where demographic data from vulnerable groups was collected, and opt-ins or opt-outs were not commonly provided options. Other concerns related to software captions instead of human captioning, issues that were subject (beyond ethical and inclusive decision-making) to human and financial resources available.

This paper reflects on these new practices in light of privacy concerns when (a) these technologies carry the potential to provide much-needed visibility and even "empowerment", and (b) these technologies are not as robust or privacy-oriented as the international organisations that include them in their everyday work with vulnerable communities. These reflections stem from the new practices being considered the "new normal" and indeed necessary for increased inclusivity. In doing so, it considers potential implications for making organisational technology applications more privacy-conscious.

Acknowledgments

This work was supported by funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 101027274. The author also gives thanks to "The Forum" for the research opportunity.

References

Madianou, M. (2020). A Second-Order Disaster? Digital Technologies During the COVID-19 Pandemic. *Social Media + Society*. https://doi.org/10.1177/2056305120948168

Milan, S., & Treré, E. (2020). The Rise of the Data Poor: The COVID-19 Pandemic Seen From the Margins. *Social Media + Society*. https://doi.org/10.1177/2056305120948233

Gilbert, D. U., & Behnam, M. (2013). Trust and the United Nations Global Compact: A network theory perspective. *Business & Society*, vo. 52, no. 1, pp. 135-169.

Newlands, G., Lutz, C., Tamò-Larrieux, A., Villaronga, E. F., Harasgama, R., & Scheitlin, G. (2020). Innovation under pressure: Implications for data privacy during the Covid-19 pandemic. *Big Data & Society*. https://doi.org/10.1177/2053951720976680

Leschanowsky A., Popp B., Peters N. (2022): Adapting Debiasing Strategies for Conversational AI. In: Proceedings of the International Conference on Privacy-friendly and Trustworthy Technology for Society – COST Action CA19121 - Network on Privacy-Aware Audio- and Video-Based Applications for Active and Assisted Living

Adapting Debiasing Strategies for Conversational AI

Anna Leschanowsky[1,2,3], Birgit Popp[2], Nils Peters[1,3]
[1]International Audio Laboratories Erlangen*, Germany
[2]Fraunhofer IIS, Germany
[3]Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany
anna.leschanowsky@fau.de,birgit.popp@iis.fraunhofer.de,nils.peters@fau.de

Abstract

Conversational AI (CAI) systems such as smart speakers or virtual assistants are widely adopted in our daily lives. While many users report privacy concerns, only few engage in privacy-protective strategies. This privacy paradox can leave users uncertain and frustrated. One explanation for the mismatch of behavior and attitudes could be that users' decision-making is subject to heuristics and biases. Debiasing strategies can help users to make rational decisions about their privacy that are aligned with their values. While nudging approaches have been applied in privacy research, little is known about other available debiasing strategies. We introduce debiasing strategies known from the medical field and show their applicability and usefulness in CAI systems.

* The International Audio Laboratories Erlangen are a joint institution of the Friedrich-Alexander-Universität Erlangen-Nürnberg and Fraunhofer IIS.

Introduction

The privacy paradox describes the discrepancy between people's attitudes towards privacy and their actual behavior and has sparked controversial debates in the field of privacy research (Kokolakis, 2017; Solove, 2021). It has been investigated in contexts such as e-commerce, social networks and CAI (Barth & de Jong, 2017; Konrad et al., 2020; Masur, 2019; Williams et al., 2017). Behavioral economics and decision research have been applied to investigate how heuristics and cognitive biases influence privacy decision-making (Acquisti, 2009). Differences in risk and benefit perception and judgement can lead users to weigh benefits higher than risks and thus engage less in privacy-protective strategies (Barth & de Jong, 2017; Leschanowsky et al., 2021). Previous research in the privacy context has shown the applicability of nudges and soft paternalism solutions as an appealing concept to improve security and privacy decisions (Acquisti, 2009).
According to Thaler & Sunstein (2008) a nudge "is any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives". Nudging approaches have been investigated in the field of mobile apps, app development and social media (Almuhimedi et al., 2015; Choe et al., 2013; Lambe et al., 2016; Wang et al., 2013). In addition, the medical field is particularly rich with empirically evaluated strategies that enable practitioners to overcome cognitive biases and avoid diagnostic errors. Thus, we will introduce four debiasing strategies known from the medical field that can improve privacy decision-making and show their applicability to CAI.

Debiasing Strategies

Checklists are a common tool to reduce cognitive failures as they provide consistency and ensure the completeness of a task. Diagnostic checklists or debiasing checklists have been investigated in the medical context resulting partly in fewer errors (Lambe et al., 2016). Usually, such checklists state possible alternative diagnoses, special diagnoses that should not be missed or provide step-by-step guidance to diagnosis (Ely et al., 2011). CAI allows the creation and management of checklists and recently a voice-controlled surgery checklist for anesthesiologists which ensures that critical safety steps are carried out has been developed (*Voice Controlled Checklist App | Softengi.Com*). A privacy-related checklist could be used to check user-specific privacy requirements before installing a new application (see Figure 1 for an example interaction). Such checklists can include items on privacy settings, can be context-dependent and present users with alternative applications. In the context of active and assisted living (AAL) technologies, privacy concerns and in particular the lack of privacy control have been shown to be one of the most prevalent barriers to acceptance

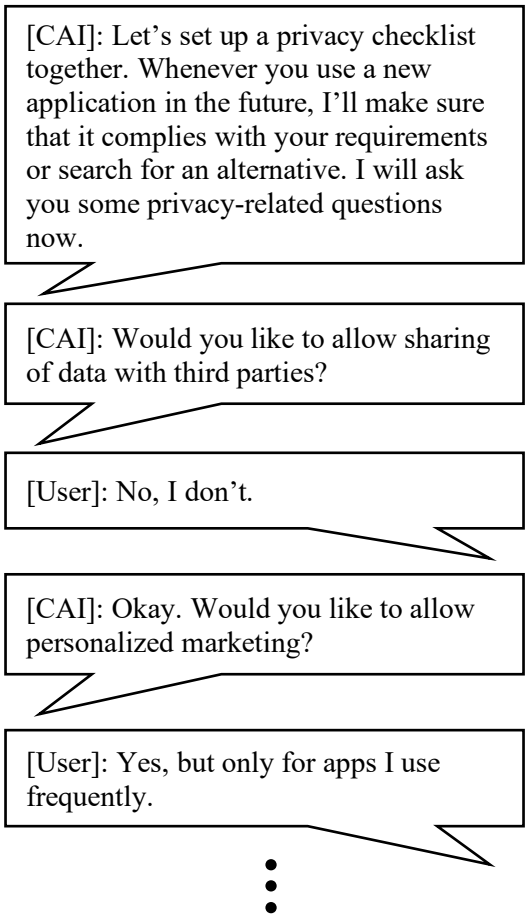


Figure 1. Example interaction for setting up a privacy-related checklist. Users can set their privacy requirements using natural language and CAI will ensure that only applications are used that comply with users' privacy requirements.

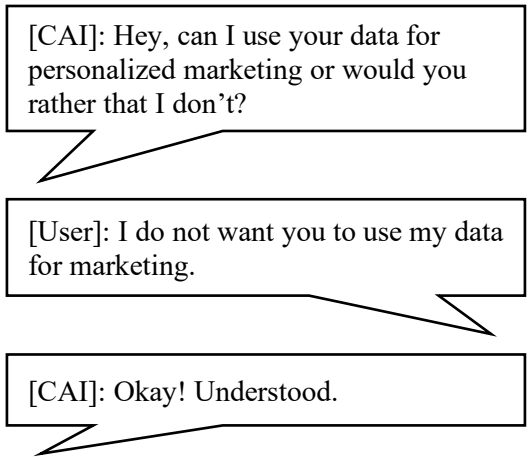


Figure 2. Example interaction using a cognitive forcing strategy where users are presented with alternative options. Considering alternatives can help users to engage in privacy decision-making that is aligned with their values. Cognitive forcing strategies can also include reconsideration of decisions.

and adoption of the technology (Jaschinski & Ben Allouch, 2019; Schomakers & Ziefle, 2019). Privacy-related checklists can allow users to easily specify data recipients, data type and frequency of transmission. Due to the conversational nature of CAI, such checklists can be set up by care receivers without dedicated technological knowledge. Nevertheless, care receivers' safety may be negatively impacted when strong control settings are applied (Jaschinski & Ben Allouch, 2019). To counter this, CAI can communicate benefits and risks of specific data transmissions and implications for safety in natural language to the users and thus, a balance between privacy and safety can be ensured.

Cognitive forcing strategies – "a specific debiasing technique that introduces self-monitoring of decisionmaking [sic!]" – can be applied to broaden clinicians' views during diagnostic processing and allow them to consider alternative diagnoses (Croskerry, 2003). While cognitive forcing strategies originated from

the medical education field, they have been applied as workplace strategies that can support clinicians at the time of decision-making (Lambe et al., 2016). It was found that when clinicians were asked to consider alternative diagnoses or reconsider diagnoses compared to diagnosing based on first impression, diagnostic accuracy increased (Lambe et al., 2016). In the privacy context, cognitive forcing strategies can be applied to support the process of rational cost-benefit analysis. Instead of making fast and intuitive decisions about disclosure or storage of one's personal information, CAI can present users with alternatives (see Figure 2 for an example interaction) or offer them the option to reconsider their decision to share data. While cognitive forcing strategies can help users to overcome their cognitive biases and consider costs and benefits more rationally, assessing costs can still be extremely difficult as privacy harms might only become apparent in the future due to new ways of data aggregation and analysis (Solove, 2012). CAI could be used to monitor data usage, inform users if necessary, and offer them the option to reconsider their decisions at the time of actual usage of their data.

Guided reflection refers to a concept in "which the practitioner is assisted by a mentor (or 'guide') in a process of self-enquiry, development, and learning through reflection" and has led to increased diagnostic accuracy when applied in the medical field (Johns, 2010; Lambe et al., 2016). The reflective practice should lead to more critical thinking of one's decision-making process. Studies on guided reflection have also used sets of procedures to diagnose a case (Lambe et al., 2016). Different to checklists where one might be reminded of possible alternative diagnoses, in studies on guided reflection participants were given detailed instruction on what to consider e.g. "list findings that support this hypothesis" (Mamede et al., 2008). In the CAI privacy context, CAI offers unique possibilities to function as a guide and to assist users in their development and privacy decision-making. Especially with the adoption of large language models such as OpenAI's GPT-3 or Meta AI's OPT-175B (Brown et al., 2020; *Meta AI is sharing OPT-175B*), CAI can be capable of acting as a guide to users that otherwise do not have access to human mentors and reflective practices. However, it needs to be ensured that language models can be trusted and that mentoring on decision-making is unbiased. Moreover, CAI could trigger reflective reasoning by asking privacy-related questions. Asking users to find and list privacy-related information themselves, could be seen as an educational strategy that raises awareness for the topic and could lead to a state where users automatically engage in reflective reasoning before disclosing personal information.

Lastly, **instructions** were used by researchers in the medical context to reduce diagnostic errors (Lambe et al., 2016). Instructions covered dual-process reasoning, a list of clinical features and thoughtful diagnosis (Lambe et al., 2016). In the CAI privacy context, instructions can be easily applied to interrupt users' intuitive decision-making and make them think more carefully about privacy decisions. For example, CAI could instruct users to consider the types of

information that are collected or ask them to think thoroughly about how their information will be used before installing a new application. While these instructions can help to overcome cognitive biases, conversational systems need to provide ways to answer possible follow-up questions from the users. Thus, similarly to easily understandable privacy labels (Kelley et al., 2009), CAI should be able to efficiently communicate privacy policies and their implications.

Conclusion and Future Work

We introduced four debiasing strategies known from the medical research field and showed their applicability and usefulness in the context of privacy and conversational AI. Debiasing strategies can support users to overcome the discrepancy between their behavior and their values regarding the disclosure of personal information. Due to the conversational and human-like capabilities and its accessibility, CAI could uniquely ensure that users engage in decision-making aligned with their values. Therefore, future research is needed to investigate debiasing techniques for privacy decision-making in the context of CAI. Moreover, debiasing strategies could not only be applied at the time of decision-making but could be used as educational strategies to raise awareness and spark discussions around the topic. Future work could consider and investigate the long-term influences of debiasing strategies on users' privacy decision-making.

References

Acquisti, A. (2009): 'Nudging Privacy: The Behavioral Economics of Personal Information'. *IEEE Security & Privacy Magazine*, vol. *7*, no. 6, 2009, pp. 82–85.

Almuhimedi, H., Schaub, F., Sadeh, N., Adjerid, I., Acquisti, A., Gluck, J., Cranor, L. F., & Agarwal, Y. (2015): 'Your Location has been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging'. in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, Association for Computing Machinery, New York, USA, 2015, pp. 787–796.

Barth, S., & de Jong, M. D. T. (2017): 'The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review'. *Telematics and Informatics*, vol. *34, no.* 7, pp. 1038–1058.

Brown, T., Mann, B., Ryder, N., Subbiah, M., Kaplan, J., Dhariwal, P., Neelakantan, A., Shyam, P., Sastry, G., Askell, A., Agarwal, S., Herbert-Voss, A., Krueger, G., Henighan, T., Child, R., Ramesh, A., Ziegler, D., Wu, J., Winter, C., Hesse, C., Chen, M., Sigler, E., Litwin, M., Gray, S., Chess, B., Clark, J., Berner, C., McCandlish, S., Radford, A., Sutskever, I., Amodei, D.. (2020): 'Language Models are Few-Shot Learners', In Larochelle, H. and Ranzato, M. and Hadsell, R. and Balcan, M.F. and Lin, H., *Advances in neural information processing systems,* Curran Associates, Inc., 2020, pp. 1877 - 1901

Choe, E. K., Jung, J., Lee, B., & Fisher, K. (2013): 'Nudging People Away from Privacy-Invasive Mobile Apps through Visual Framing'. In P. Kotzé, G. Marsden, G. Lindgaard, J. Wesson, & M.

Winckler, *Human-Computer Interaction – INTERACT 2013*. Springer Berlin Heidelberg, 2013, pp. 74-91

Croskerry, P. (2003): 'Cognitive forcing strategies in clinical decisionmaking'. *Annals of Emergency Medicine*, vol. *41, no.* 1, pp. 110–120

Ely, J. W., Graber, M. L., & Croskerry, P. (2011): 'Checklists to Reduce Diagnostic Errors'. *Academic Medicine*, vol. 86, no. 3, 2011, pp. 307–313

Jaschinski, C., & Ben Allouch, S. (2019): 'Listening to the ones who care: Exploring the perceptions of informal caregivers towards ambient assisted living applications'. *Journal of Ambient Intelligence and Humanized Computing*, vol. *10, no.* 2, pp. 761–778.

Johns, C. (2010). *Guided reflection: A narrative approach to advancing professional practice* (2nd ed). Johns, C. Blackwell Pub.

Kelley, P. G., Bresee, J., Cranor, L. F., & Reeder, R. W. (2009): 'A „nutrition label" for privacy'. In *Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS '09*, Association for Computing Machinery, New York, USA, 2009, pp. 1 - 12

Kokolakis, S. (2017): 'Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon.' *Computers & Security*, vol. *64*, 2017, pp. 122–134.

Konrad, M., Koch-Sonneborn, S., & Lentzsch, C. (2020): 'The Right to Privacy in Socio-Technical Smart Home Settings: Privacy Risks in Multi-Stakeholder Environments'. In C. Stephanidis & M. Antona (Hrsg.), *HCI International 2020—Posters*, Springer International Publishing, pp. 549 - 557

Lambe, K. A. O'Reilly, G., Kelly, B. D., & Curristan, S. (2016): 'Dual-process cognitive interventions to enhance diagnostic reasoning: a systematic review'. *BMJ quality & safety*, vol. 25, no. 10, 2016, pp. 808–820.

Leschanowsky, A., Brüggemeier, B., & Peters, N. (2021): 'Design Implications for Human-Machine Interactions from a Qualitative Pilot Study on Privacy'. *2021 ISCA Symposium on Security and Privacy in Speech Communication*, pp. 76–79

Mamede, S., Schmidt, H. G., & Penaforte, J. C. (2008): 'Effects of reflective practice on the accuracy of medical diagnoses'. *Medical Education*, vol. *42*, no. 5, 2008, pp. 468–475.

Masur, P. K. (2019): *Situational Privacy and Self-Disclosure: Communication Processes in Online Environments* (1st ed. 2019). Springer International

Meta AI is sharing OPT-175B, Retrieved May 13 2022, from https://ai.facebook.com/blog/democratizing-access-to-large-scale-language-models-with-opt-175b/

Schomakers, E.-M., & Ziefle, M. (2019): 'Privacy Perceptions in Ambient Assisted Living', In *Proceedings of the 5th International Conference on Information and Communication Technologies for Ageing Well and E-Health*, SCITEPRESS - Science and Technology Publications, Crete, Greece, 2019, pp. 205–212

Solove, D. J. (2021): 'The Myth of the Privacy Paradox'. *89 George Washington Law Review 1 (2021), GWU Legal Studies Research Paper No. 2020-10, GWU Law School Public Law Research Paper No. 2020-10*

Solove, D. J. (2012): 'Privacy Self-Management and the Consent Dilemma', *Harvard Law Review,* vol. 126, no. 7, 2012, pp. 1880 - 1903

Thaler, R. H., & Sunstein, C. R. (2008): '*Nudge: Improving decisions about health, wealth, and happiness'*. Yale University Press.

Voice Controlled Checklist App | softengi.com., Retrieved February 24, 2022, from https://softengi.com/projects/voice-controlled-checklist-app/

Wang, Y., Leon, P. G., Scott, K., Chen, X., Acquisti, A., & Cranor, L. F. (2013): 'Privacy Nudges for Social Media: An Exploratory Facebook Study', In *Proceedings of the 22nd International Conference on World Wide Web* (*WWW '13 Companion*). Association for Computing Machinery, New York, NY, USA, 2013, pp. 763–770.

Williams, M., Nurse, J. R. C., & Creese, S. (2017): 'Privacy is the Boring Bit: User Perceptions and Behaviour in the Internet-of-Things', *15th Annual Conference on Privacy, Security and Trust (PST)*, 2017, pp. 181–18109.

William Dutton, Grant Blank, Egle Karpauskaite (2022): Who Cares about Privacy Online? In: Proceedings of the International Conference on Privacy-friendly and Trustworthy Technology for Society – COST Action CA19121 - Network on Privacy-Aware Audio- and Video-Based Applications for Active and Assisted Living

Who Cares about Privacy Online?

William Dutton, Grant Blank, Egle Karpauskaite
Oxford Internet Institute, University of Oxford, UK
william.dutton@gmail.com, grant.blank@gmail.com,
egle.karpauskaite@oii.ox.ac.uk

Privacy advocates argue that websites are capable of automatically compiling copious amounts of information on individuals without their knowledge. As data are collected and used without the user's knowledge, privacy is increasingly threatened. Others have questioned some privacy concerns, arguing that alarmists do not understand the limited value of data collected for particular applications.

Despite such debates, governments have begun to develop regulatory measures to address internet-created dangers to privacy. One response is the EU's General Data Protection Regulation, which requires individuals give permission for their data to be collected. In addition, the GDPR grants rights such as the right "to be forgotten", the ability to have personal data removed from a database. To protect privacy, the GDPR assumes an omni-capable citizen, one who has the knowledge, resources, and time to protect their privacy online.

While policymakers pass legislation to grant privacy rights to citizens, the extent to which citizens share their concerns is unclear. To what extent are people concerned and willing to act to protect their data online? This paper is based on the quantitative analysis of survey research and explores the enigma surrounding privacy attitudes and actions.

The first part of the paper explores the levels of concern over digital privacy and whether the attitudes are related to the demographic characteristics of the individual. The second part of the paper discusses the "privacy paradox" – the inconsistency of attitudes towards privacy and privacy behavior. Using logistic regression analysis, we examine how concern over privacy relates to whether people actively protect their personal information online.

Our analyses use data collected for the Oxford Internet Survey (OxIS), a representative sample of the British population. Surveys were completed in 2009, 2011 and 2013. Most of our analyses use the most recent wave which was completed in 2019. The dependent variable is responses to whether individuals believe that "Use of computers & the Internet threatens personal privacy". Response categories were a 5-category Likert scale ranging from "Strongly disagree" to "Strongly agree".

OxIS data shows that concern over privacy has increased by about 10 percentage points in the past decade. Between 2009 and 2019 the share of respondents who "agreed" or "strongly agreed" that internet is a threat to privacy rose from 45% to 55%

In the second part of the paper considers the relationship between privacy concern and privacy-related behavior. There are significant associations between perceiving internet as a threat to privacy and taking steps to keep private age, relationship status, medical condition, and shopping habits . However, privacy concerns do not seem to move individuals to take steps to protect their contact details.

These preliminary findings show that individuals are increasingly concerned with their privacy online. Those worried about their privacy tend to take steps to secure some pieces of personal information but not all personal data. On one hand, taking preventative measures might have an inverse effect on privacy attitudes – those taking steps to secure their privacy feel less concerned. On the other hand, several preventative measures seem to have no association with privacy concerns. While digital privacy concern is growing, the relationship between concern and behavior is not clear. The findings suggest rethinking existing privacy legislation. As individuals are inconsistent with attitude and behavior, the assumption of an omni-capable citizen is unrealistic.

Belani, H., Fišter, K., and Šolić, P. (2022): Acceptability of m-Health Solutions and its Relationship with Public Trust. In: Proceedings of the Int. Conference on Privacy-friendly and Trustworthy Technology for Society – COST Action CA19121 - Network on Privacy-Aware Audio- and Video-Based Applications for Active and Assisted Living

Acceptability of m-Health Solutions and its Relationship with Public Trust

Hrvoje Belani[1], Kristina Fišter[2], Petar Šolić[3]
[1] Ministry of Health, Directorate for e-Health, Ksaver 200a, 10000 Zagreb, Croatia
[2] University of Zagreb, School of Medicine, Šalata 3, 10000 Zagreb, Croatia
[3] University of Split, Faculty of Electrical Engineering, Mechanical Engineering and Naval Architecture, Ruđera Boškovića 32, 21000 Split, Croatia
hrvoje.belani@miz.hr; kfister@snz.hr; psolic@fesb.hr

Abstract

Mobile devices with health-related apps hold the potential for increasing the quality and efficiency of healthcare services. Two years of the COVID-19 pandemic have put additional stress on already struggling healthcare systems around the world, representing an opportunity for digital tools and e-health solutions to step in. This paper analyses acceptability of three mobile health solutions in Croatia and its relationship with public trust. Each of the apps, Health Portal, Stop COVID-19 and CovidGO, had their own paths to the users, paved by provided information, promotion existence and dynamics, as well as the impact of public actions, such as media appearances of authority figures mentioning the apps. Health Portal and Stop COVID-19 apps gained momentum as well as the national uptake of EU digital COVID certificates, for which CovidGO app was instrumental. Needing to use one app, users realized there are other m-health apps published by the Ministry of Health at the global app stores, which many chose to download as well. This demonstrates a certain level of citizens' trust to the offered solutions.

Introduction

The United Nations 2030 Agenda for Sustainable Development (UN, 2015) emphasizes that "the spread of information and communications technology (ICT) and global interconnectedness has great potential to accelerate human progress, to bridge the digital divide and to develop knowledge societies". World's population using the Internet since 2019 until 2021 increased by 17%, representing 782 million people estimated to have come online during that period and resulting in approximately 4.9 billion people or 63% using the Internet, mostly covered by a mobile-broadband signal (ITU-D, 2021). Therefore, global usage of mobile devices with health-related apps represents a great potential for increasing the quality and efficiency of healthcare services, also overcoming barriers to access, which has been recognized as one of the permanent challenges for health systems worldwide.

The World Health Organization (WHO) defines mobile health or m-health as a component of electronic health or e-health (WHO, 2011) and a "medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs), and other wireless devices". The WHO Executive Board has also defined digital health as "often used as a broad umbrella term encompassing e-health as well as developing areas such as the use of advanced computing sciences (in the fields of big data, genomics and artificial intelligence, for example)" (WHO, 2017).

When it comes to assessing health interventions, including digital ones (e. g. m-health), acceptability has been defined within the theoretical framework of acceptability (TFA) as a "multi-faceted construct that reflects the extent to which people delivering or receiving a healthcare intervention consider it to be appropriate, based on anticipated or experienced cognitive and emotional responses to the intervention" (Sekhon et al., 2017). TFA consists of seven component constructs: affective attitude, burden, perceived effectiveness, ethicality, intervention coherence, opportunity costs, and self-efficacy.

Research on technology acceptance go more than three decades back. The Technology Acceptance Model (TAM) and TAM2 deal more specifically with the prediction of the acceptability of an information system determined by two main factors: perceived usefulness and perceived ease of use (Davis et al., 1989). The Unified Theory of Acceptance and Use of Technology (UTAUT) and UTAUT2 explain and predict the acceptance of technology firstly in an organizational context (Venkatesh et al., 2003), with many later additions and evolution of these models.

While both models aim at understanding better why users accept or reject a given technology, and how user acceptance can be improved through technology design, recent reviews show that "TAM and UTAUT failed to provide stable predictive capabilities for acceptance and use of technologies in health care" (Ammenwerth, 2019), with possible reasons specific for healthcare, where technology acceptance is influenced by socio-organizational and cultural factors.

Motivation and related work

With global spread of SARS-CoV-2 and the COVID-19 pandemic outbreak at the beginning of 2020, the usage of digital tools for enabling healthcare and related services gained in importance to patients as well as health professionals globally. Before the pandemic, "the greatest barriers to adoption of digital health tools were not primarily technical in nature, but instead lay in successfully facilitating the required individual, organizational and system changes" (Fahy and Williams, 2021). The same report recognizes four main areas digital health tools have been used during the pandemic: "support four main areas: communication and information, including tackling misinformation; surveillance and monitoring; the continuing provision of health care such as through remote consultations; and the rollout and monitoring of vaccination programs".

However, countries rushed deployment and adoption of such solutions raises profound concerns about surveillance, privacy and data protection. The case study (Newlands et. al., 2020) on digital surveillance technologies implemented during the COVID-19 pandemic delineates "the contextual nature of privacy trade-offs during a pandemic" exploring "how regulatory and technical responses are needed to protect privacy in such circumstances". The same study stated, "greater effort in incorporating privacy considerations beforehand in the design of digital solutions is very much needed, as afterthought privacy reflections risk exposing the health of citizens, wasting public resources and worsen the consequences that the state of emergency already has for society".

National health systems, such as the one in Croatia (Capak et al., 2020), as well as international collaborative initiatives, such as the eHealth Network of the European Union (eHealth Network, 2022), have increasingly developed and launched digital health tools in response to COVID-19. The European Commission (EC) and the EU member states have worked together to improve the efficiency of contact tracing and warning apps in 2020 and have defined a common approach for uniform and interoperable proofs of vaccination, testing, and recovery from COVID-19 via EU Digital COVID Certificates (EU DCC) in 2021. For the later, detailed technical specifications of the trust framework have been worked on jointly and reference implementations published as an open source. Clear trust framework allowed many (40, until end May 2022) third countries to join the EU DCC system.

This paper provides an insight in acceptability of three m-health apps implemented by Croatia. m-Health in Croatia is defined by the Healthcare Act ("The Official Gazette", No. 100/2018, 125/2019, and 147/2020) as "the use of mobile devices to collect medical and public health data. The application of m-health implies the use of mobile communication devices for the collection of general and clinical health data, the transfer of health information to physicians, researchers and patients, and remote monitoring of medical parameters of the patient".

Methods and tools

The first three m-health apps published and upgraded by the Croatian Ministry of Health during 2020 and 2021, as shown in Fig. 1, on two of the biggest mobile apps platforms (stores) worldwide, Google Play and App Store, were the following:

- Health Portal – Croatian patient portal app, providing citizen's access to personal health data from the electronic health records (EHR), among others: COVID-19 vaccination and testing records, making a COVID-19 vaccination appointment, messages exchange with the chosen doctors, lists of e-prescriptions dispensed and e-referrals issued, as well as medical reports received from primary care laboratories and specialists,

- Stop COVID-19 – Croatian COVID-19 warning and exposure notification app, for anonymous exchange of random encrypted strings via Bluetooth Low Energy (BLE) protocol, fetching the list of strings from infected persons, processing the data in a decentralized manner – on the device in order to find a match and solidary warn the contacts of the infection risk,

- CovidGO – Croatian EU DCC verifying app, with functionalities of reading and decoding QR codes from the COVID certificates and verifying the digital signature of the issuer, as well as the wallet for safe storage of EU DCCs. The app is cross-border interoperable for fetching signature keys.

When the timeline of all three m-health apps releases (launches) and major upgrades have been analyzed, along with other public actions, compared to the apps download statistics from Google Play (Android), as shown in Fig. 1, it can be seen that each of the apps have the unique path. Only Google Play (Android) download statistics have been used for the analysis, because it has shown sufficient for recognizing trends, as approx. 84% of app users are Android users.

The insightfulness of such an analysis depends of how many public actions have been pointed out, which served as triggers for statistics numbers to change course or dynamics. One of the public actions had been the health minister promoting "Stop COVID-19" app on November 19, 2020, which caused significant increase in the app' downloads.

In order to assess the acceptability of these official Croatian m-health solutions, a short online survey using Google Forms has been prepared with five questions on demography and seven questions on the use of mobile devices and m-health apps. The survey questions focused only of perceived and experienced usefulness, not covering the other aspects provided by the TAM/TAM2 or UTAUT/UTAUT2 models. The survey results have been shown in Fig. 2 and Fig. 3. and detailed in the next section.

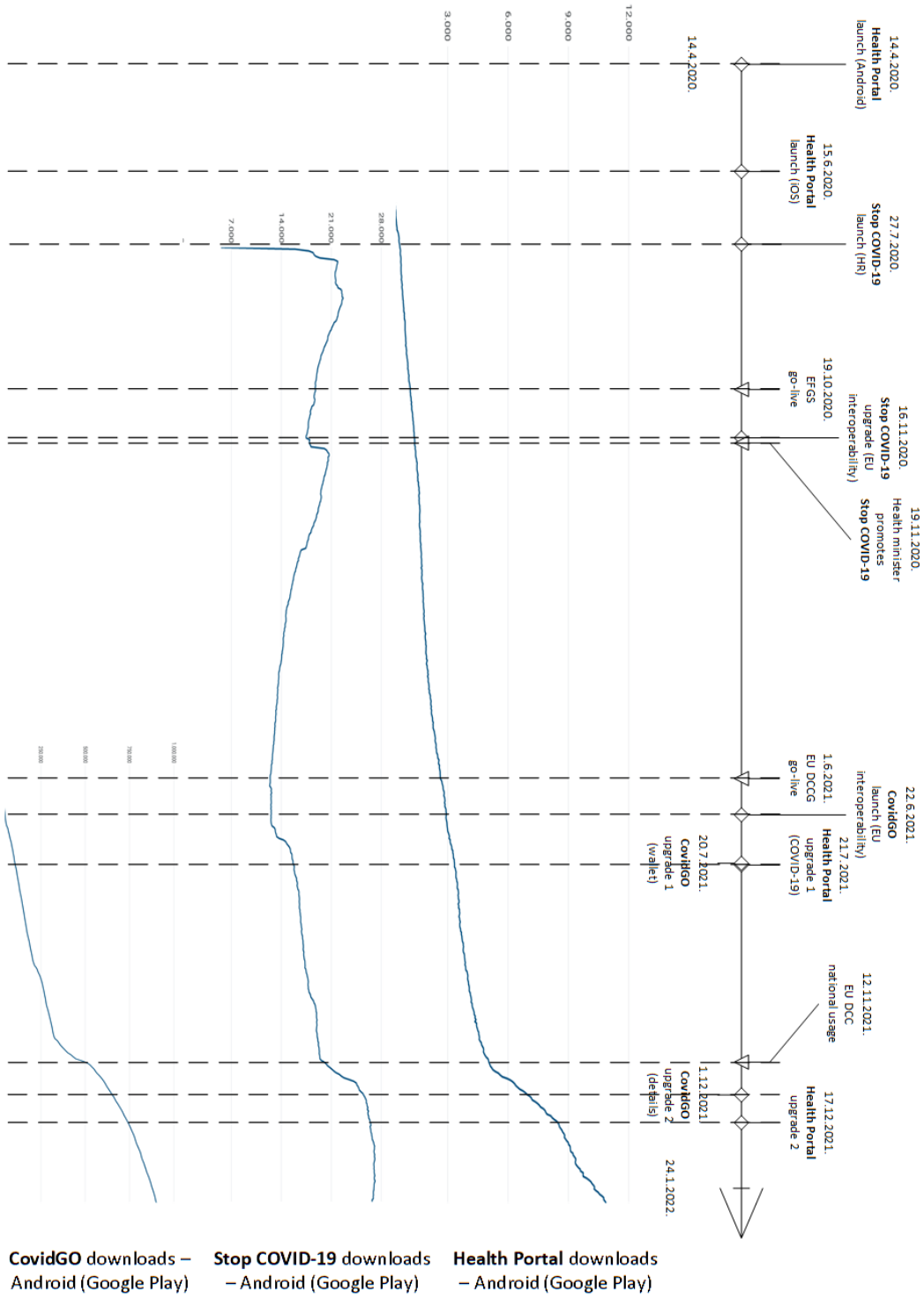


Figure 1. The timeline of the m-health apps releases (launches) and major upgrades, along with other public actions, compared to the apps download statistics from Google Play (Android).

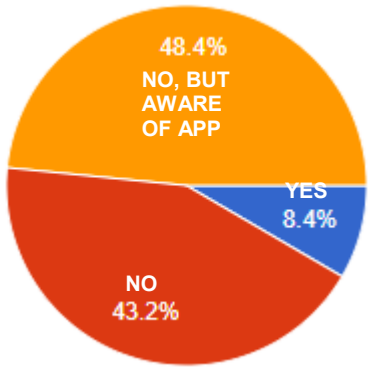
Results and discussion

The online survey was active from November 30, 2011 until January 24, 2022, 55 days in total, and was presented to three cohorts of respondents from the University of Zagreb:

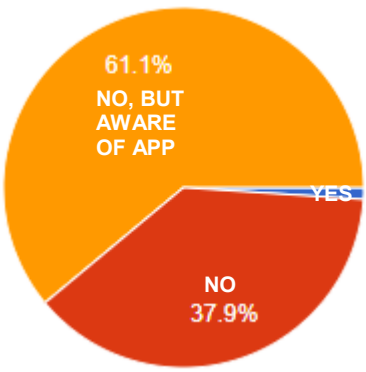
- 2nd year's graduate students of EE and computer science attending Biomedical Informatics course at the Faculty of EE and Computing,
- 3rd year's graduate students of pharmacy attending Pharmaceutical Informatics course at the Faculty of Pharmacy and Biochemistry,
- 1st year postgraduate specialist students of epidemiology from Medical Informatics course at the School of Medicine.

The results of the 95 responses showed that almost 98% of respondents owned a mobile phone capable of using the apps from the stores. Around 2/3 of respondents were female, while 1/3 were male. Regarding the age group distribution, 63.2% of respondents were 21-25 years old, 17.9% were 16-20, 8.4% were 31-40, 7.4% were 26-30, 2.1% were 41-50 and 1% were 51-60.

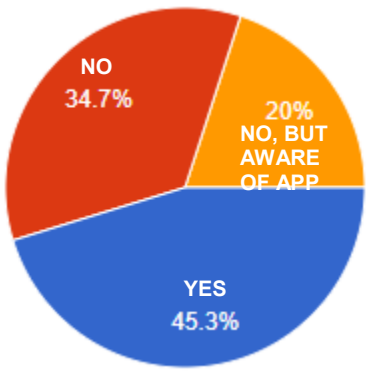
a) Do you own a smart phone?



b) Have you installed Health Portal app?



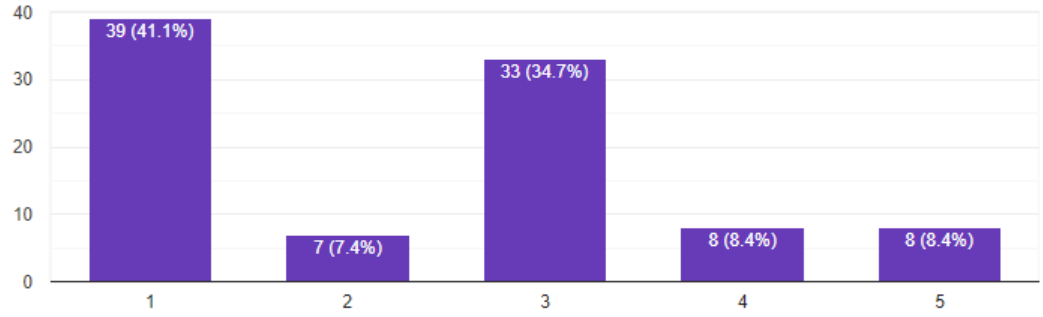
c) Have you installed Stop COVID-19 app?



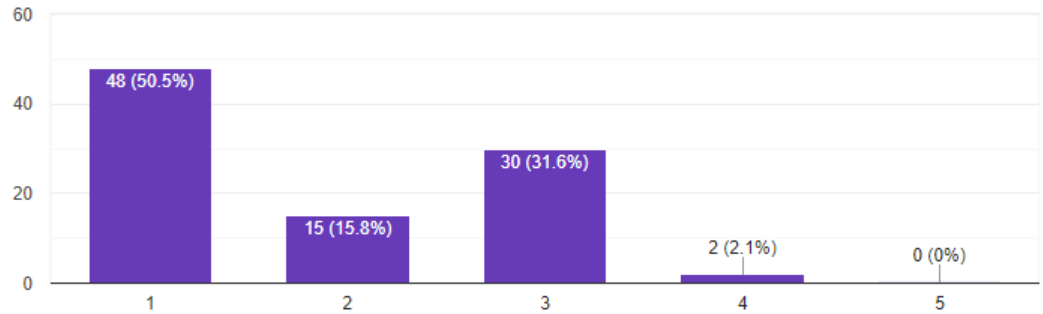
d) Have you installed CovidGO app?

Figure 2. The survey answers (N=95) about owning a smart phone and installing m-health apps.

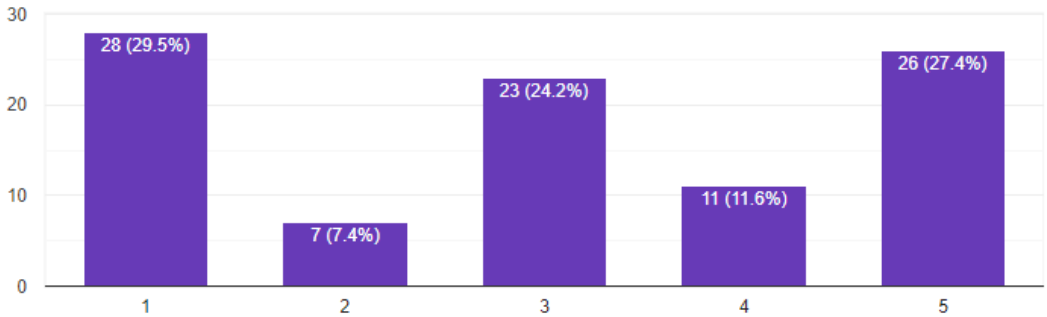
As the survey answers show in Fig. 2, around 2/3 of respondents were aware of CovidGO app and 45.3% of them installed it, which makes sense because the app has been regularly promoted in the media and among citizens affected by the need to use EU DCCs for crossing the EU borders and later even nationally. Health Portal app was installed by 8.4% of respondents, without any organized public promotion, but being an additional user interface to the existing web application known to citizens. The least installations (1%) were done with Stop COVID-19 app, without any public promotion at all and with some bad publicity non-justifiably lagging from before launching the app when the public trust was lost.



a) How much have you found Health portal app useful? (1 – not at all; 5 – completely useful)



b) How much have you found Stop COVID-19 app useful? (1 – not at all; 5 – completely useful)



c) How much have you found CovidGO app useful? (1 – not at all; 5 – completely useful)

Figure 3. The survey answers (N=95) about the degree of usefulness of the apps (Likert scale).

Survey answers in Fig. 3 support the ascertainment that CovidGO app has been found as the most useful to respondents (with 3 points average). Health Portal app was somewhat useful to respondents (with 2.4 points average), while Stop COVID-19 app was found not much useful to respondents (with 1.9 points average).

Conclusion

Although all three apps had dedicated web pages (Health Portal, 2020) (Stop COVID-19, 2020) (EU DCC, 2021), those were not instrumental in gaining public trust. Health Portal app had a steady, organic growth in acceptability by the users during 2020 and 2021. Stop COVID-19 publicity was damaged before the app was launched, due to efforts by the authorities to propose legislative changes that would allow launching a quarantine management app and consequent concerns over intrusion to user privacy. Appreciable uptake of CovidGO app was guided by the decisions of the Civil Protection National Headquarters, authorized by the law to introduce epidemiological measures and restrictions during COVID-19 pandemic.

References

Ammenwerth E. (2019): 'Technology Acceptance Models in Health Informatics: TAM and UTAUT," *Studies in health technology and informatics*, *263*, pp. 64–71. https://doi.org/10.3233/SHTI190111.

Capak, K., Kopal, R., Benjak, T., Cerovečki, I. Draušnik, Ž., Bucić, L., Pristaš, I. Curać, J. (2020): 'Surveillance system for coronavirus disease 2019 epidemiological parameters in Croatia', Croat Med J. 2020;61:481-2, https://doi.org/10.3325/cmj.2020.61.481

Davis, F., Bagozzi, R., and Warshaw, R. (1989): 'User Acceptance of Computer Technology: A Comparison of Two Theoretical Models', Management Science, Volume 35, 1989, pp. 982-1003.

eHealth Network: 'eHealth and COVID-19', EC - Directorate-General for Health and Food Safety (DG SANTE), Retrieved April 8, 2022 from https://ec.europa.eu/health/ehealth-digital-health-and-care/ehealth-and-covid-19_en

'EU Digital COVID Certificate (EU DCC)', Published on June 1, 2021, Ministry of Health, Ministry of Interior, Croatia, Retrieved April 8, 2022 from https://www.eudigitalnacovidpotvrda.hr/

Fahy, N. and Williams, G. A. (eds) (2021): 'COVID-19 Health System Response Monitor Network', Policy Brief 42, 37p, European Observatory on Health Systems and Policies, ISBN: 1997-8073.

'Health Portal (Portal zdravlja)', Published on September 9, 2016, Ministry of Health, Croatia, Retrieved April 8, 2022 from https://portal.zdravlje.hr/portalzdravlja/index.html

ITU-D (2021): 'Measuring digital development, Facts and figures 2021', International Telecommunication Union, Geneva, Switzerland, Retrieved April 8, 2022 from https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2021.pdf

Marikyan, D. & Papagiannidis, S. (2021): 'Unified Theory of Acceptance and Use of Technology: A review'. In S. Papagiannidis (Ed), TheoryHub Book. http://open.ncl.ac.uk

Newlands, G., Lutz, C., Tamò-Larrieux, A., Villaronga, E. F., Harasgama, R., & Scheitlin, G. (2020): 'Innovation under pressure: implications for data privacy during the Covid-19 pandemic', Big Data & Society, 7(2), 2053951720976680.

Sekhon, M., Cartwright, M., Francis, J. J. (2017): 'Acceptability of healthcare interventions: an overview of reviews and development of a theoretical framework', BMC Health Services Research 17, No. 88(2017), https://doi.org/10.1186/s12913-017-2031-8.

'Stop COVID-19', Published on July 27, 2020, Ministry of Health, Croatia, Retrieved April 8, 2022 from https://stopcovid19.koronavirus.hr/

UNDESA (2015): 'Transforming our world: the 2030 Agenda for Sustainable Development', The United Nations Division for Sustainable Development Goals, Retrieved April 8, 2022 from https://sdgs.un.org/2030agenda

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012): 'Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology', MIS Quarterly, 36(1), 157–178, https://doi.org/10.2307/41410412

WHO Global Observatory for eHealth (2011): 'mHealth: New horizons for health through mobile technologies: second global survey on eHealth', World Health Organization, Geneva, Switzerland, Retrieved April 8, 2022 from https://apps.who.int/iris/handle/10665/44607

WHO Executive Board, 142. (2017): 'mHealth: use of appropriate digital technologies for public health', Report by the Director-General, World Health Organization, Retrieved April 8, 2022 from https://apps.who.int/iris/handle/10665/274134