Building User Trust of Critical Digital Technologies

Thomas Given-Wilson
Universite Catholique de Louvain
Louvain-la-Neuve, Belgium
thomas.given-wilson@uclouvain.be

Eduard Baranov
Universite Catholique de Louvain
Louvain-la-Neuve, Belgium
eduard.baranov@uclouvain.be

Axel Legay
Universite Catholique de Louvain
Louvain-la-Neuve, Belgium
axel.legay@uclouvain.be

***Abstract*—Digital technology is permeating all aspects of human society and life. This leads to humans becoming highly dependent on digital devices, including upon digital: assistance, intelligence, and decisions. A major concern of this digital dependence is the lack of human oversight or intervention in many of the ways humans use this technology. This dependence and reliance on digital technology raises concerns in how humans trust such systems, and how to ensure digital technology behaves appropriately.**

This works considers recent developments and projects that combine digital technology and artificial intelligence with human society. The focus is on critical scenarios where failure of digital technology can lead to significant harm or even death. We explore how to build trust for users of digital technology in such scenarios and considering many different challenges for digital technology. The approaches applied and proposed here address user trust along many dimensions and aim to build collaborative and empowering use of digital technologies in critical aspects of human society.

I. Introduction

Digital technology is permeating all aspects of human society and life. This covers a broad range of technologies and areas, with human society using digital technology for day-to-day entertainment and communication, to relying upon digital technology for key infrastructure, transport, and healthcare. This pervasive integration of digital technology into human society increasingly leads to humans becoming highly dependent upon digital technology.

Digital technologies now provide assistance, intelligence, and decisions in many areas of human society aiding [3], [14], guiding [5], [14], [19], or even informing humans on how to act [15]. A major concern of this digital dependence is the lack of human oversight and understanding of how some digital technologies may operate [15]. There is also the potential for conflict when humans and digital technologies conflict [9], [15], which can lead to fatal results [9]. This dependence and reliance upon digital technology requires that humans are able to trust such digital systems and their behavior so as to allow effective usage of this technology without conflict.

This work considers recent developments and projects that combine digital technology and artificial intelligence with human society. The focus is on critical scenarios where digital technology is involved with healthcare and vulnerable humans who may rely upon digital technology in matters of safety, dignity, and even with their life. We explore how to build trust for users of digital technology in such scenarios and considering many different challenges for digital technology. For these areas we highlight some challenges for user trust, and also consider how recent and ongoing projects address this requirement for humans to be able to trust digital technologies. In particular we highlight how trust must be addressed along multiple dimensions that interrelate, and that these must be addressed in design, implementation, and human integration.

The structure of the paper is as follows. Section II overviews the projects and some key scenarios for user trust of digital technologies. Section III identifies some key challenge areas where user trust must be established. Section IV highlights approaches that can be used to build user trust in these challenge areas. Section V discusses and concludes.

II. Scenarios

This section overviews the key goals of three projects where digital technology is used to assist and empower humans. The first is the ACANTO project where vulnerable adults used digital robotic assistants for medical treatment recovery and mobility assistance [3]. The second is the Serums project that focuses on how to improve digital technology for medical records across borders and data analytics while also empowering patients [17]. The third is the Wablieft project where a digital marketplace is used to improve delivery of medical services.

One of the main goals of the ACANTO project is to provide adults with limited mobility an assistive robot (as shown in Fig. 1), called a *FriWalk*, that can assist with diagnostics and medical treatments as well as help with navigation [3],

Fig. 1: Prototype FriWalk used in trials with sensors exposed.

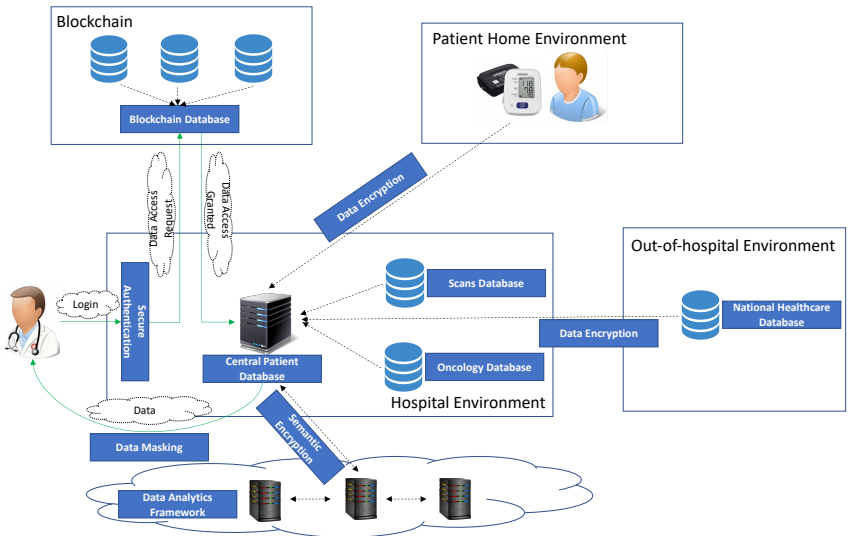

Fig. 2: Serums key component overview.

[5], [10], [20]. The user of a FriWalk may depend upon the FriWalk for diagnosis, treatment plans, physical support and navigation, and thus the user has dependencies upon the FriWalk, particularly when in an environment where the user could not navigate or move freely without the FriWalk [10].

The overall goal of the Serums project is to enable the sharing of medical information across borders to ensure effective treatment across administrative regions while empowering users to maintain control of their medical data [17]. A high level overview of key components of Serums is shown in Fig. 2. The includes access by medical professionals, patients, and data analytics to various data sources that make up a patient record. Serums users are to opt into making their medical record available for access in other regions as required (not shown), but also allowing users to then have fine-grained control over the access to and usage of their medical record. Optionally patients may also allow their medical record or specific information therein to be used for data analytics and medical research.

The aim of the Wablieft project is to create a secure digital marketplace for medical services. Like Serums, to allow usage of the Wablieft marketplace requires that medical information about patients and medical services be communicated and used in Wablieft. The goal of this digital marketplace is to improve the efficiency and access of medical services, while empowering users to also consider their own preferences and not just follow those of a single nominated provider.

Another aspect with significant impact on these digital systems that handle personal information is developments in societal expectations and legal requirements. One significant development is the implementation of *General Data Protection Regulation* (GDPR) [2] that puts strong restrictions on how personal information is used and who owns or controls this information. This is particularly pertinent to digital technologies such as in the Serums and Wablieft projects since patients must always be able to know how their medical data is used, and have control over who has access to their data and under what circumstances.

III. Trust Challenges

For users to be confident and willing to use critical digital technology, the users must have a high level of trust in the technology itself [4], [13]. This trust can vary significantly according to what the digital technology provides even within the field of healthcare; e.g. the trust required of a doctor's desktop computer is still very different to that of a digital pacemaker. Thus while trust varies considerably, with the increase in dependence upon digital technology, the level of trust required, particularly for highly sensitive digital technology, is significant. This section discusses four challenge areas for user trust that emerge due to digital technologies and their adaptation.

A. Medical Practitioners Engagement

One challenge for any new technology when it concerns critical information is how to build trust in new users of the technology and to build a base of users to support further development and use of the technology [6]. Thus, for users to be comfortable and trust a new digital technology it is important for the digital technology to have support from experts within the field, here medical practitioners.

In ACANTO, since the FriWalk aims to be a diagnostic and treatment capable medical device (among other capabilities), the willingness of doctors and nurses to use the device and be convinced of it's utility and safety is critical to adoption.

In Serums the challenge for engagement by medical practitioners is more complex since the scope of the project is significantly larger and involves many more parties. Thus, the engagement needs to involve medical practitioners from multiple locations and jurisdictions to ensure the overall goals and focus of the project is maintained. Indeed, to have utility beyond a digital medical record and local data analytics, the Serums digital technologies must be adopted by multiple medical facilities.

In Wablieft the scale of adoption and engagement is also much more complex, albeit with interesting and competing dynamics. If the marketplace provides an effective way to find treatments then this will be useful for doctors and also treatment providers. However, there is the complexity of the marketplace as well, since a marketplace with no or only one provider will not be able to provide much benefit over current systems. Thus, the engagement for Wablieft must involve many treatment providers to be effective, as well as doctors willing to rely upon these services.

To build trust for patients as users of all three projects, the trust and engagement of their medical service practitioners is critical. In particular, if a patient's doctor recommends a digital technology then this is likely to be accepted and trusted by patients much more than without such a recommendation.

B. Access Control

One key challenge for user trust is to be confident that access to the digital system (and the information within it, medical or otherwise) is correctly handled and controlled [11].

In ACANTO the FriWalk devices store medical diagnostic information that should only be accessed by a medical practitioner, and in particular a practitioner treating the FriWalk user (patient). Thus, control of who has access to this medical data is critical to certification and patient trust. For the social use of the FriWalk, access control concerns who has access to the navigation goals and sensor information of the FriWalk.

In Serums the challenge of access control is much more significant since patient records need to be widely accessible within medical practice, and further one of the goals of Serums is to allow cross-border access [17]. This raises many challenges regarding how to control access to ensure that the patient medical record is available to: the patient, their (nominated) doctor(s), and paramedics (potentially from another country in an emergency) to give a few examples. Further, within Serums the goal is not only to support access where this can save lives, but also to limit access to only pertinent and appropriate information.

In Wablieft challenges are similar to the those of Serums. The patient and their doctor must have access, while limited access is also necessary for the service provider and marketplace (to check if patient is eligible for service). In the latter case it must be ensured that only necessary information can be accessed.

One complication particularly for Serums and Wablieft is the GDPR requirements, since these imply that patients must have final ownership and thus control over who can and has accessed their data. Thus, access control in [ractice must implicitly also allow for various parties to be able to modulate the access and also keep records of this access in a secure and tamper-proof manner.

C. Privacy & Information Leakage

Another challenge that is exacerbated in digital technologies is the leakage of privacy or information through indirect means [18]. While a user or patient may agree to allow their information to be stored or used, there are always concerns about lack of privacy, anonymity, or other leakage of private information [18].

User privacy related to participation is common among all three projects. The participation risk is that by using digital technology the information that someone is a user may be revealed. In a general sense, this is a common risk to many areas and so the challenge is to ensure that merely using digital technology does not leak information about user participation.

In ACANTO the navigation assistance uses information about traffic and the environment that is gathered from the user, other users, and environmental sensors [3], [10]. This sharing of location and sensor information means that information can be leaked about the presence of a FriWalk user, and potentially their travel history or other location information [10]. For example, a FriWalk is able to react to avoid collision with a pedestrian that is around a corner and out of sensor range by using sensor information from another FriWalk.

In Serums the other main challenge for information leakage is related to the use of patient information for aggregate analytics [17]. One goal in Serums if to be able to mine patient records (for users who have opted in) to perform data anlytics and discover improvements for healthcare treatments and services. The use of aggregate data requires that patient information is anonymised, masked, or even handled in a manner that prevents significant risk to the user of their information being related to them [1], [8], [21], i.e. that the data is de-anonymised.

In Wablieft the main challenge is to ensure that open information from marketplace cannot lead to the leak of information about the users, to ensure that the treatment history or the illness is not revealed. This concerns both ensuring that the identity of a patient in the Wablieft marketplace is protected from accidental leakage, and also that even participation cannot be inferred.

D. Predictability

A significantly different kind of challenge to user trust in digital systems is the predictability of the digital technology [16]. It is important for users to feel that the system behaves in a manner that they can reasonably see is within expectations and predictions of what the digital technology should provide.

In ACANTO this predictability is significant since the user may rely upon the FriWalk to provide navigation assistance. While the FriWalk may at times choose different paths when considering different traffic or environmental factors, the user must have confidence that the navigation is reasonable and not wildly unpredictable, or significantly worse than the navigation the user themselves would choose while trusting that the FriWalk has equal or better knowledge about the environment.

In Serums the predictability is mostly related to how the user's information is made available, or whom, and how this information can be used. Since GDPR and Serums require users to have control over how their data is accessed and used, this requires that the behavior of the system is predictable based upon the permissions given by the users. Another

area is in the data analytics, where users of data mining on Serums data must be able to trust that the data they receive is adequately anonymised.

In Wablieft the main challenge to predictability is in the handling of the marketplace behavior. The user must trust that when they use the marketplace to find a treatment, they are being offered correct treatments and also those that are a good choice. The counter-point would be if the user discovered they were not offered the service that matched their requirements or the service description is missing important information, since this would degrade their trust in using the marketplace for treatments in future.

IV. Approaches

This section considers how these challenges can be addressed and how this can build trust between the user and digital technology. Observe that many of these approaches and challenges are inter-related, and improving one can build trust in another. For many of these challenges, the approach combines both a design aspects of the approach, and implementation aspects to ensure the design is achieved.

A. Medical Practitioners Engagement

To address medical practitioner engagement requires the involvement and feedback of medical practitioners to ensure the digital technology is embraced and understood by the experts who will use or recommend the digital technology in future. This section highlights how each project approaches this engagement.

ACANTO is more advanced than the other projects and has had significant time to engage and develop with medical practitioners. This took the form of involving medical experts from a hospital in the project to guide the medical utility of the FriWalk and the overall ACANTO project goals [3]. During the project doctor feedback was taken into the design of the FriWalk (both hardware and software). Later in the project the FriWalk was certified as a trial medical device, and a pilot study was conducted with doctors and patients to not only evaluate the effectiveness of the digital technology, but also the impact on patients both physically and mentally, as well as feedback from the doctors conducting the treatments [20]. Both doctors and patients reacted positively to the FriWalk and patient outcomes were improved [20].

In Serums the engagement is more complex since the project aims to engage many more kinds of medical practitioners and from more diverse backgrounds [17]. To assist with this, the Serums project involves medical practitioners from three different medical facilities in three different countries [17]. At this stage of the Serums project feedback has been gathered from medical practitioners in two medical facilities in different countries and this is being integrated into the design and development of Serums digital technologies.

Wablieft involves several different actors making the engagement more difficult. It is planned (Wablieft is at early stage) to run a small scale experiment involving medical practitioners, treatment providers and patients to gather feedback and expectations to help design and develop the system.

To build trust for patients as users of all three projects, the projects involve medical practitioners and service providers as part of the project. The goal of this is to engage and include the medical practitioners in the design of digital technology, and to ensure the outcomes are aligned with the requirements and expectations of medical practitioners, as well as to build ownership of medical practitioners in these digital technologies.

B. Access Control

One critical challenge for digital technologies that handle critical information is the control of who has access to the system and in what manner. Here this is both granting and preventing access to the digital technologies, since in these projects access to some information is critical for health and safety, while also now being bound by legal complications such as GDPR.

In ACANTO the main method to ensure controlled access of medical information is to only allow medical practitioners the ability to access the data on the FriWalk. Since the FriWalk is designed and certified as a medical device with access restrictions implemented, this provides an easy solution.

Of more interest is the Serums access control since the patient records at the heart of Serums require complex access control to be useful and also meet legislative requirements. To manage this, Serums digital technologies are built with fine-grained user-controllable access control policies based on smart contracts. These smart contracts allow the construction of rules that apply to access of patient records and components within them. Thus, it is possible for a patient record's general information to be visible to all medical practitioners within the hospital the patient is currently being treated in, but for specific test results or even details of treatments to only be available to pertinent medical staff. It is possible for a patient record's general information, such as name and allergens, to be visible to all medical practitioners within the hospital the patient is currently being treated in, but for specific test results or even details of treatments to only be available to pertinent medical staff, for example the blood test available only to oncologist.

To safeguard the above controls Serums smart contracts are used and all access rules and authorizations are maintained on a blockchain (learning from [7]) shared among different medical facilities. This design allows the sharing of access and information between facilities, e.g. for when a user has an emergency in a foreign country and critical information such as allergies can be extremely important to obtain. This also ensures that no individual facility can uniquely control or change the access records, ensuring trust between facilities and for users who know that a data breach or illegal data access cannot be simply hidden by a single compromised entity.

In Serums formal and statistical methods are being used to validate that the design of the smart contracts are feasible and do not allow for incorrect or malicious behavior. These approaches are also being applied to the authentication system, and to the implementation to validate that the Serums project is not vulnerable to malicious data access.

The Wablieft access control approach is similar to Serums, with a formal approach to defining the marketplace access policies. Access to patients data is planned to be controlled allowing to see the details for the patient and his doctor, while this information would not be shared with the marketplace and treatment providers, only identification information might be accessed. In order to check the eligibility for buying a service, medical practitioners would define several groups based on illnesses and distribute services between them. The patient data would be enhanced with the list of groups the patient associated with (can be modified only by patient's doctor) and an API would be provided for the marketplace to request whether the user belongs to a particular group.

In Wablieft, similar to Serums, formal methods and statistical approaches are proposed to be used for validation of design and implementation correctness.

C. Privacy & Information Leakage

The challenge of effectively preventing the leakage of private information in digital technologies requires more technological solutions, since traditional policies and approaches tend to be vulnerable to vast computing resources and easy access to vast amounts of data.

In ACANTO participation is visually obvious since the FriWalk device cannot be obviously hidden, thus the challenge for participation is related only to preventing knowledge of participation by access to data gathered by a FriWalk. This is simply mitigated by the access control policy (see Section IV-B) that prevents access except for doctors who would be granted this information anyway.

The navigation aspects of the ACANTO project include communication between FriWalk devise to allow for improved navigation and safety of users. This is similar in practice to sharing traffic information between cars on a shared road system. Here the ACANTO design requires some location information or environment knowledge to be shared, in particular to inform on traffic congestion and obstacles that may lead to collisions. Although this is in some sense anonymous (and may be further anonymised [10]), in practice some information must be leaked since otherwise collisions may occur. In practice information can come from many potential sensors from many locations, and so precise information about the true location of another FriWalk user can be obscured.

In Serums the potential to leak participation information is non-trivial. On one hand, by following existing policies regarding confidentiality of patient participation and storage of medical records this already meets current requirements and expectations. On the other hand, one of the goals of Serums is to provide medical data more freely for travelers or people who suffer a medical emergency away from their home medical services. Considering the latter, in Serums the existence of a patient's record is made available based on guidelines that take input from medical policies, governments, and of course patients. These are being gathered to design a formal specification of when access to a record, and thus potential leakage of the record's existence, can be allowed. The result here will be a formal specification of when patient information can be revealed, and in particular one in which the patient has final control.

Once this specification is formalised, verification and validation technologies will be applied to the implementation and formalisation to ensure that the policy does not have any errors in design, and that the implementation matches this formal specification. This in turn provides formal guarantees about the security of the system, and in particular about the inability to leak information.

Another area in Serums is when a user's medical data is used as part of a larger data analytics for improving treatments. Here the goal in Serums is to be able to use machine learning on the medical information, at least on records where the user has given permission for their information to be anonymously used for research purposes. To ensure that users are not de-anonymised in any sense, in Serums the differentially private data analytics and machine learning are implemented [8], [12] built into their construction. This will ensure that no individual user's record is provably part of the data being used, and so no individual user could be proved to have participated [12].

In Wablieft the participation problem is non-trivial. To ensure predictability IV-D the marketplace activity is stored on a blockchain which could allow to gather private information. Therefore, all such information is decided to store in a separate space with a proper access control, while leaving only anonymised information in the blockchain. There is an ongoing work on formalisation of requirements and their validation and verification to guarantee non-existence of leaks.

D. Predictability

To help build user trust the digital technologies considered here must be predictable and reasonable for their users.

In ACANTO this predictability is significant in the navigation assistance provided by the FriWalk to the user. Here careful design and implementation decisions were made to ensure that the navigation assistance acts in a "human" manner and provides "human-like" navigation suggestions [5]. This requires some delicacy in the case of ACANTO as in navigation the varying environment can lead to navigation choices that may not seem obvious without complete information, e.g. avoiding a busy area that the user cannot see may appear to send the user via a less optimal route. In ACANTO this is also improved by the assistive nature of the FriWalk that will cede to the user's choice, and if the user follows other navigation decisions than the FriWalk re-plans accordingly.

In Serums the predictability is required to consider both the users as patients and the users as medical practitioners. For patients the rules used to allow their access, as well as any default behaviors, must be made simple to create. To ensure no unexpected conflicts or behavior can occur, validation and verification (see Sections IV-B & IV-C) ensure that the rules will be followed by the digital technologies in Serums. From the medical practitioners side there must be a little more delicacy since this can be contrary to privacy and information leakage concerns. For example, a doctor who attempts to look

up test results for a patient may find no records due to: the patient not existing, the patient deleting their record, the doctor not having access to the patient record at all, or the doctor not having access to that specific test result. Further to the example, it may be delicate to inform the doctor of which situation they are in, since being blocked by the patient may be something the doctor should not be aware of. Thus, while the correctness of the implementation can be validated at the implementation level, some further research is ongoing into how to handle the various cases for all users of the Serums digital technology in a manner that addressed the various challenges here.

In Wablieft, the predictability is required for patients and treatment providers. Patients expect a booked service to be received and of good quality while treatment providers expect fair and correct functioning of the marketplace. To achieve these, the activity of the marketplace would be recorded in a blockchain which immutability would allow to ensure the correctness of work of the marketplace, e.g. no double use of a service, as well as to evaluate the quality of the treatment provider based on its history. There is an ongoing research on the information stored in blockchain to allow this while preserve the privacy. Validation and verification would be used to ensure correctness of the marketplace functioning.

V. Discussion & Conclusions

The ACANTO, Serums and Wablieft projects all involve the integration of critical digital technology into human lives and society. These projects consider scenarios where the human users of digital systems are often at their most vulnerable, and when the digital systems handle some of the most private and intimate of user information. Thus, for successful adoption and use of these digital technologies, it is vital that the users trust the digital technologies.

To build trust between users and digital technologies it is necessary to consider and address many challenges. Here these are consider in many dimensions, and with their inter-related effects on trust and how to design and implement digital technologies that will be trustworthy to their users. This work has highlighted examples including: engagement and adoption from medical practitioners; controlling access to critical medical information; maintaining user privacy and preventing information leakage; and predictability of digital technologies. In each area we give examples of where trust needs to be built, and discuss the approaches (to be) taken in these projects to build user trust.

More broadly this work illustrates the complexities of digital technologies and how to develop them in a manner that garners user trust. In particular this work illustrates the many dimensions that need to be considered, and also how they inter-relate with one-another to collectively build and ensure user trust of a digital technology.

References

[1] Article 29 data protection working party, independent european advisory body on data protection and privacy. opinion 05/2014 on anonymisation techniques, April 2014.

[2] Regulation (eu) 2016/679 (general data protection regulation). http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679, 2016.

[3] ACANTO project web site. http://www.ict-acanto.eu/, October 2019.

[4] L. Alzahrani, W. Al-Karaghouli, and V. Weerakkody. Analysing the critical factors influencing trust in e-government adoption from citizens' perspective: A systematic review and a conceptual framework. *International Business Review*, 07 2016.

[5] P. Bevilacqua, M. Frego, D. Fontanelli, and L. Palopoli. Reactive planning for assistive robots. *IEEE Robotics and Automation Letters*, 3(2):1276–1283, 2018.

[6] D. L. Boeldt, N. E. Wineinger, J. Waalen, S. Gollamudi, A. Grossberg, S. R. Steinhubl, A. McCollister-Slipp, M. A. Rogers, C. Silvers, and E. J. Topol. How consumers and physicians view new medical technology: Comparative survey. *J Med Internet Res*, 17(9):e215, Sep 2015.

[7] J. P. Cruz, Y. Kaji, and N. Yanai. Rbac-sc: Role-based access control using smart contract. *IEEE Access*, 6:12240–12251, 2018.

[8] C. Dwork. Differential privacy. In *33rd International Colloquium on Automata, Languages and Programming, part II (ICALP 2006)*, volume 4052 of *LNCS*, pages 1–12. Springer Verlag, July 2006.

[9] German Federal Bureau of Aircraft Accidents Investigation. Investigation report ax001-1-2 (english). http://www.bfu-web.de/EN/Publications/Investigation%20Report/2002/Report_02_AX001-1-2_Ueberlingen_Report.pdf?__blob=publicationFile, May 2004.

[10] T. Given-Wilson, A. Legay, and S. Sedwards. Information security, privacy, and trust in social robotic assistants for older adults. In *Human Aspects of Information Security, Privacy and Trust - 5th International Conference, HAS 2017, Held as Part of HCI International 2017, Vancouver, BC, Canada, July 9-14, 2017*, pages 90–109, 2017.

[11] V. Kisekka and J. S. Giboney. The effectiveness of health care information technologies: Evaluation of trust, security beliefs, and privacy as determinants of health care outcomes. *J Med Internet Res*, 20(4):e107, Apr 2018.

[12] M. Kumar, M. Rossbory, B. A. Moser, and B. Freudenthaler. Deriving an optimal noise adding mechanism for privacy-preserving machine learning. In G. Anderst-Kotsis, A. M. Tjoa, and I. Khalil, editors, *Database and Expert Systems Applications*, pages 108–118, 2019.

[13] J. McMurray, G. Strudwick, C. Forchuk, A. Morse, J. Lachance, A. Baskaran, L. Allison, and R. Booth. The importance of trust in the adoption and use of intelligent assistive technology by older adults to support aging in place: Scoping review protocol. *JMIR Res Protoc*, 6(11):e218, Nov 2017.

[14] L. Palopoli, A. Argyros, J. Birchbauer, A. Colombo, D. Fontanelli, A. Legay, A. Garulli, A. Giannitrapani, D. Macii, F. Moro, P. Nazemzadeh, P. Padeleris, R. Passerone, G. Poier, D. Prattichizzo, T. Rizano, L. Rizzon, S. Scheggi, and S. Sedwards. Navigation assistance and guidance of older adults across complex public spaces: the dali approach. *Intelligent Service Robotics*, 8(2):77–92, Apr 2015.

[15] A. Pritchett and E. Fleming. Pilot compliance to tcas resolution advisories. pages 1–23, 10 2013.

[16] J. Reinhardt, A. Pereira, D. Beckert, and K. Bengler. Dominance and movement cues of robot motion: A user study on trust and predictability. In *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pages 1493–1498, Oct 2017.

[17] SERUMS project web site. https://serums-h2020.weebly.com/, October 2019.

[18] M. Sokolova and S. Matwin. *Personal Privacy Protection in Time of Big Data*, pages 365–380. Springer International Publishing, Cham, 2016.

[19] A. J. Spiers and A. M. Dollar. Design and evaluation of shape-changing haptic interfaces for pedestrian navigation assistance. *IEEE Transactions on Haptics*, 10(1):17–28, Jan 2017.

[20] M. Valdés-Aragonés, P. Moreno, R. Pérez-Rodríguez, M. Oviedo-Briones, S. Walter, N. García-Grossocordon, and L. Rodríguez-Mañas. Acanto project: recruitment description on elderly admitted into geriatrics departments through the use of a robotic friendly walker. *14th Congress of the European Union Geriatric Medicine Society*, 2018.

[21] J. Zhang, Y. Zhao, Y. Yang, and J. Yang. A k-anonymity clustering algorithm based on the information entropy. In *Proceedings of the IEEE 18th International Conference on Computer Supported Cooperative Work in Design, CSCWD 2014, Hsinchu, Taiwan, May 21-23, 2014*, pages 319–324, 2014.