SELF-MONITORING DEVICE IMPLEMENTATION DURING COVID-19

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Wayne Wong

Spring 2022

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Rider W. Foley, Department of Engineering and Society

Introduction

With the technological progress towards a fully automated world becoming a closer reality with wearables and other self-monitoring technologies being constantly integrated into today's society, the socio-technical effects of the health-oriented monitoring technology are becoming increasingly more important to study. To simplify things, the devices being studied will be broken up into two categories: monitoring devices for medical use and monitoring devices for personal or commercial use. However, with both types of health-monitoring technology, improper device design for target social groups, civilian technical illiteracy, and the risk of security breaches regarding medical information have prevented these devices from gaining the expected popularity over the past twenty years (Graham, 2020). Both medical and commercial technologies have had integrational issues over this time, but some outliers have broken into the realm of commonly accepted and used devices (Yassein, 2019). Consequently, a socio-technical deep dive into these devices, their integration, and the legislation around them is required to understand the effects that come from the adoption of this technology and what can be done to integrate health-oriented monitoring devices more successfully.

The primary concern that arises from self-monitoring technology, specifically health-related, is privacy and what happens with the data. According to a 2019 PEW Research study, it was found that 81% of United States (U.S.) adults feel that they have a lack of control over the data that companies collect (Auxier, 2020). Along with this, 79% of U.S. adults are concerned about how companies are using and protecting the data that is collected (Auxier, 2020). To emphasize this point, U.S. HIPPA standards do not cover companies creating medical self-monitoring technologies which open a sharing loophole for these corporations (Gerke, 2020). Along with this, the Food and Drug Administration (FDA) expressed that any app or software

service with the intent of public health surveillance of COVID-19 spread and symptoms did not fall under the FDA's jurisdiction of medical devices (Health, 2020). The lack of sufficient HIPPA and FDA regulations demonstrates a legal loophole that gives significant merit to the American concerns regarding the privacy of their medical and health-related data. Along with this, during the COVID-19 pandemic, further federal regulatory policies were dropped for these self-monitoring devices due to the time of crisis which led to additional privacy and safety concerns (Gerke, 2020). Due to the significance of both the safety and privacy of the target demographics, I will be analyzing multiple notable health-related technologies developed during the COVID-19 pandemic under the ISTA framework to pinpoint the socio-technical shortcomings of these devices.

Case Context

To obtain data that covers the entirety of the thesis, there will be two primary groups of technologies studied: consumer self-monitoring technology used for COVID-19 tracing and remote medical databasing of new monitoring technology. For the consumer self-monitoring technology, the primary focus will be on COVIDWise and COVIDSafe, two applications for mobile devices that allow local Bluetooth transmissions from nearby devices to alert users of being a close contact. Since these applications were created with the intent of being used by the entirety of a population for maximum effectiveness, there is not much of a target consumer demographic that it could be improperly engineered for. However, improper design of the technological infrastructure for use by medical personnel directly impacted them as an actor in the network created by these devices. The privacy aspect regarding the large-scale socio-technical effects of improperly protected medical data is much greater due to the scale of the

availability, access, and usage of mobile devices. The data from these companies is privately managed meaning the standards in place to protect user data are not as sufficient as with existing medical infrastructure which must follow HIPAA standards. All of this allows for the exploration into the legislation regarding the company's accessibility and marketability of this data and to explore the legal, as well as moral, guidelines that are in place to protect the user's best interest and who's burden that is.

In contrast to the consumer-integrated devices mentioned above, it is also important to consider the devices that are designed for medical usage. Since there are additional privacy guidelines in place when dealing with medical information in a hospital, the privacy concern is slightly more limited due to HIPPA guidelines regarding patient discretion. However, for the medical portion, the demographic issue becomes more prominent. Since these monitoring technologies generally need to be more focused on a certain age group or people with a specific medical condition, the target demographic and the effects of the group are easier to identify. For this, the technology that will be analyzed will be two monitoring systems that were implemented during the COVID-19 pandemic to monitor patient symptoms from a distance, or in some cases even at home. Data collected regarding overall satisfaction and concerns with implementation from surveys and case studies would provide good contrast in comparison with the consumer health tracking devices. Along with this, a useful comparison to relate the two would be regarding privacy. Since HIPAA regulations are stricter than base legislation regarding data security and privacy with patient data, it should give good guidelines for how other medical data should be handled by companies.

With the more specific HIPAA regulations not focused on external companies creating self-monitoring devices to be integrated into existing HIT, it would be expected that the FDA

would manage the data privacy concerns and safety aspects of these devices. However, this is not the case. On March 26, 2020, the FDA released a statement saying that “The FDA does not consider most apps and software systems for public health surveillance and communication to be medical devices regulated by the FDA” (Health, 2020). This means that any mobile handling of private medical data that was handled through a software or an application would not need to be verified by the FDA, unlike other medical devices which tend to require extensive testing measures (Health, 2020). Unfortunately, the technology that fell under this statement included various applications implemented during the COVID-19 era that monitored user private data was not being verified to have the same security and privacy that has become a standard for medical technology.

Interactive Sociotechnical Analysis

Since these health-related self-monitoring technologies integration is what I am interested in, I will use Interactive Sociotechnical Analysis (ISTA) to analyze the devices and observe the socio-technical effects that come from each of the points for observation. Since the focus is on both the device and the background interfacing and integrating, ISTA provides a near-perfect framework to discuss the technology and its effects on the different actors of each technology. ISTA gives a good baseline for these new medical technologies because it focuses on the integration process into existing socio-technical systems as well as the independent environments themselves (Harrison, 2007). This will be specifically targeted with the first two types of interactions and the unintended consequences that came from each interaction. The first of these interactions would be regarding the changes in Healthcare Information Technologies (HIT) that change an existing social system. For this area, the new COVID-19 devices will be used for the

analysis because of the necessity to integrate them as fast as possible due to the pressing nature of the disease and the severe effects that many people suffered. Since the whole integrational process was necessary, the devices and the interfaces changed the existing social system of face-to-face care. The second point of analysis is when technical and physical infrastructures mediate HIT. This can be analyzed from the point of view of the integration of COVIDWise and COVIDSafe onto Apple and Google devices as they both use existing infrastructure to mediate the health monitoring device and interface. The socio-technical effects can be observed in the quick integration of Apple and Google's Bluetooth tracking systems into existing devices to both monitor health statistics and close COVID-19 exposures. For gaps left with ISTA, actor network theory can be used because it provides a broader view of the networks and allows for the specific evaluation of individual actors, humans, and nonhumans, instead of overall groupings (Latour, 1992). Both frameworks being used together should allow for the construction of a good socio-technical skeleton to evaluate the effects of the integration of these self-monitoring health devices, both medical and commercial.

Research Question and Methods

The question that drove the research for this paper was, how did new monitoring technology developed during the COVID-19 pandemic affect United States citizens and healthcare workers concerning implementation strategies, overall user safety, and privacy concerns? With existing privacy and safety loopholes in HIPAA and the FDA existing simultaneously but separately for medical monitoring devices, the COVID-19 pandemic provided a first look into the device integration through the combination of these policies. To explore the interaction of the devices in new or existing HIT networks, two case studies were

observed to understand the privacy and safety effects for actors in the network. The first case that was examined was a study performed by Sara Gerke, which examined the regulatory, safety, and privacy concerns of home monitoring technologies during the COVID-19 pandemic. This one was chosen to examine a broadscale view of the policies that changed regarding self-monitoring health technologies and frame the safety and privacy hazards that arose from such changes. The second case that was looked at was a study by Florian Vogt, who looked into the effectiveness of COVID-19 digital contact tracing. This was chosen as the sole case study at the time of writing with tangible effectiveness data of a COVID-19 self-monitoring device that can be examined underneath the ISTA frameworks with additional inspections into data privacy from Gerke's case study. The cases were both broken down and analyzed using the following steps: 1) demonstrate the relevance of the case to the ISTA framework, 2) describe the results found in the case, and 3) analyze the socio-technical effects experienced by the actors from the results.

Findings

After examining both the case studies, it was determined that the combination of the existing legislature and new statements from the FDA and Secretary of Health and Human Services permitted unsafe practices and put patients' private medical information in danger, as seen in Figure 1. Loosened regulations of the testing from the FDA and the Emergency Use Authorization (EUA) declarations allowed for companies producing COVID-19 monitoring devices to bypass regulations that assure patient data privacy that is ordinarily enforced by HIPAA. The EUA declarations encouraging technology to be rolled out faster came at the cost of effectiveness and user safety as well.

Event	Effect on Data Privacy
August 21, 1996: HIPAA Enacted	- Does not include a statement regarding externally managed data privacy - Does not restrict data usage or enforce privacy standards that would be assumed in the medical field
February 4, 2020: U.S. Secretary of Health and Human Services declares Emergency Use Authorization Declarations for Multiple Monitoring Devices	- Allows for external products to bypass ordinary safety testing to get products out faster - Products on market are introduced that were focused on speed, not privacy concerns
March 26, 2020: FDA finds public health surveillance software during COVID-19 not under jurisdiction	- Determined the U.S. government had no jurisdiction over large scale data collection by companies during the COVID-19 era, as monitoring applications did not fall under the category of medical devices.

Figure 1. Major Data Privacy Events that Affected the Implementation of Health-Related Self-Monitoring Devices During the COVID-19 Pandemic

Outsourced Data Handling in Times of Crisis

The first interaction point of ISTA that is essential for interpreting the new self-monitoring health devices of the COVID-19 era is regarding the changes of HIT that change an existing social system (Harrison, 2007). Due to the unknown nature and fast spread of the virus, many legislative changes needed to be made to assist in the development of technology to combat the difficulties of healthcare in isolation. Of these, Sara Gerke focused on the EUA

declarations and the shortcomings of HIPAA when dealing with third-party data privacy concerns.

On February 4, 2020, the U.S. Secretary of Health and Human Services (HHS) determined that the spread of COVID-19 in the United States was grounds for the declaration of three EUA declarations (Gerke, 2020). One of these three broadly included alternative products that can be used as medical devices, including home monitoring devices (Gerke, 2020). Of these, the primary example that will be addressed will be a EUA that was issued to G Medical Innovations for a patch that is intended to allow for remote patient monitoring of vitals and possible side effects of the virus (Gerke, 2020). The data is then collected via the patient's smartphone and sent to a certified cardiographic technician before being sent to the doctor at the hospital (Gerke, 2020). Although outsourcing the innovation and database management to outside companies may be the best thing to do in terms of speed, it brings with it a slew of data privacy and safety concerns.

When it comes to patient data privacy, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) is the base guideline used for the United States. While the act has done a sufficient job of keeping patients' health records private, the COVID-19 pandemic and EUAs regarding medical devices have created a loophole. The HIPAA privacy rule currently only applies to health information only if it is generated by "covered entities", including most healthcare providers and business associates (Gerke, 2020). Since most technology companies fall outside of HIPAA's scope, data that is gathered from independent companies is not bound by any of the privacy regulations, normally enforced by HIPAA (Gerke, 2020). Along with this, the Office for Civil Rights at HHS announced in April of 20202 that it will not enforce possible HIPAA violations against business associates' use or disclosure of protected health information.

This “blind spot” for outsourced technology companies impacts the actors of the network in two specific ways. The first of these is in terms of the overall privacy that is assumed of the healthcare industry because of assumed HIPAA standards. The second of these is regarding the overall accessibility and issues that come with adding an unrestricted party to the health industry.

With the healthcare sector already at a heightened vulnerability to cyberattacks, outsourcing technology development to outside companies with limited data privacy restrictions negatively can impact patients. With data breaches already becoming a more commonplace issue in society, implementing technology that uses outside databasing adds significant vulnerability to patients’ valuable health data. Along with this, with HIPAA data breaches and cyber security attacks being reported by 47% of organizations in 2017, there is a legitimate need to assure data security when outsourcing to an external company (Snell, 2017). Therefore, although speed was a necessity when developing this technology, the voiding of any data disclosure punishments for EUAs and the lack of any privacy guidelines for these companies cause major privacy vulnerabilities for the healthcare network and its patients (Murdoch, 2021). An example of this can be seen with the COVID-19 Bluetooth contact tracing which tracks Bluetooth signals from nearby smartphones. This location data along with the health status of individuals is an instance of sensitive data that would ordinarily be regulated under HIPAA. This adds another element of insecurity to an already fragile data management system and needs to be further regulated.

Outsourcing patient private data creates additional issues for healthcare workers trying to treat their patients to the highest level of care while putting sensitive patient data at risk. When the data is not handled within the established healthcare infrastructure, there is an inherent concern regarding data access issues when utilizing a third party (Brumen, 2013). Merely the presence of an additional external company adds further opportunity for data vulnerabilities and

cyberattacks on top of the fact that medical situations require data access in a timely matter (Snell, 2018). Therefore, any sort of server issues from one of the unregulated companies would have severe negative effects on health care professionals' ability to treat patients with the highest level of care. Thus, the implementation of COVID-19 self-monitoring technologies creates additional safety and privacy risks for both the patients and health care workers, with the only real benefit coming to the external companies.

Bluetooth-Driven Contact Tracing

When looking into the second point of ISTA regarding how new technical and physical infrastructures mediated HIT during the COVID-19 pandemic, a primary example would be smartphone companies' implementation of contact tracing apps into their devices (Harrison, 2007). The case study that was examined for this was the Australian research study performed by Florian Vogt that performed an evaluation of the effectiveness of digital contact tracing of the COVIDSafe app between May 4 and November 4, 2020 (Vogt, 2022). Despite the U.S. utilizing a slightly different application, COVIDWise, the overall design was near-identical since both used the duration, frequency, and transmission strength of neighboring Bluetooth emissions to determine possible contacts (Vogt, 2022). Since Bluetooth-driven contact tracing was created as a new HIT, the interactions between it and the existing HITs already in use mean that it can be addressed concerning the second point of ISTA.

Through the six months of data collection, 619 confirmed COVID-19 cases and 25,300 close contacts were observed with COVIDSafe being used in 137 cases, which resulted in 205 contacts (Vogt, 2022). Out of these, only 79 of these contacts met the criteria of being a close

contact, giving a positive predictive value of 39% (Vogt, 2022). The COVIDSafe app was also found to only have an estimated sensitivity of 15% further discrediting the actual effectiveness of this style of mobile contact tracing (Vogt, 2022). Furthermore, the development of the app ended up costing around $230,000 with additional monthly payments of $29,000 per month for maintenance (Sanchez, 2020). Despite the cost being relatively low to taxpayers, the effects could be further felt within the public health system.

The issues regarding the overall effectiveness of Bluetooth contact tracing effects can be seen through almost all actors in the network. The primary group of these to address is the users of the application. Although the notification system for possible close contact's cellular devices is significant in that it alerts of any possible exposures, the error margin and discovered ineffectiveness of these apps can lead to a false sense of security or panic among people regarding a deadly virus. With a 39% positive predictive value and a measly 15% estimated sensitivity, the question arises of whether a technology with such a weak predictability metric is helping prevent cases or furthering the spread through undetected false negatives. This can be seen as a design failure that could and should be found by the FDA or Department of Health and Human Services due to its overall ineffectiveness and safety concerns. The fast design and quick implementation of Bluetooth COVID-19 contact tracing that was permitted through the lack of regulatory legislature generated an additional workload and dataset for health care staff to interact with, therefore increasing the opportunity cost of the whole device.

Even though the application over-predicted close contacts, which isn't necessarily bad for stopping the spread of COVID-19, the effects of isolation for false-positive close contacts were significant, specifically for low-income families. Despite the Family First Coronavirus Response Act requiring paid leave for COVID circumstances, it only applied for two weeks of

professionally advised self-quarantine (Department of Labor, 2020). With 61% of the U.S. population living paycheck to paycheck, any additional necessary isolation, due to false contact tracing, would put this demographic under greater financial stress (Dickler, 2022). The existing financial stress already felt by the lower economic class would only be increased with additional and incorrect close contact evaluations from the barely functional software. Therefore, due to the lack of consistent data accuracy presented to the users, the difficult interfacing for health care workers, and the general cost of maintenance, the rushed Bluetooth contact tracing caused more negative socio-technical effects on the actors than benefits.

Discussion

After utilizing the methodology with the two cases studies, two primary takeaways came from both. First, there is inherent insecurity with the addition of external cloud-based large data systems and lax HIPAA regulations regarding medical self-monitoring technology that deteriorates the previously existing data security of the status quo. The second takeaway was that the lack of effectiveness of some technologies and outsourced companies can cause inaccuracies which can negatively affect the quality of care for all patients by adding or altering infrastructure that does not integrate well into existing social systems.

The research performed on the two cases with the ISTA framework shows the significant unintended consequences regarding the actors in the healthcare network. However, due to the nature of the state of emergency during the implementation of these devices, the responsibility for the negative side effects becomes confusing. With two primary parties, third-party companies and the U.S. government, bearing most of the decisions for the designs and implementation of

these devices, I believe that a deontological breakdown could be performed. An interesting question arises on whether it is the U.S. government's responsibility to assure the people's data privacy or if it is within the engineer's code of ethics to create something that does not endanger the users. I believe that this responsibility to regulate third-party medical technology companies primarily falls on HIPAA. Although FDA classification of such software and devices as medical devices would be beneficial for required testing, HIPAA defines the guidelines for patient data privacy. However, in theory, if the engineers followed the code of ethics and never released any technology that did not meet ethical standards regarding privacy or safety, this would also solve the problem. Mistakes can be made without specific data regulations in place that the engineers should be held accountable for. I believe that tightening these HIPAA guidelines would prevent the faulty or insecure devices from being integrated into the HIT.

Along with this, the state of emergency changes some aspects when it comes to the utilitarian perspective on the situation. Since the COVID-19 crisis was a critical issue during the majority of 2020, a solution to the problem was a necessity. An argument could be made on whether the benefit of these technologies, despite them not being regulated by HIPAA standards, outweighed the negative side effects that came because of it. Since most of the negative implementation effects were risk and endangerment while the benefits were tangible, I believe that a utilitarian look at this could vary from what was determined from the research.

Limitations and Caveats

Due to the complex situation of the COVID-19 pandemic concurrently with its recency, there were many limitations when analyzing some of the case studies. First, the state of

emergency of the pandemic makes it difficult to analyze some of the decisions of the government and companies in the development process. This changes risk assessment during this period, and it is easy to look at the situation in retrospect and examine where the decisions could have been incorrect. The most specific case for this comes with the argument of endangering private data. Since patient data was in danger, not because of the engineers or design, but the way data and privacy laws affect healthcare companies makes it a more complex issue in what could have been changed.

Future Considerations

Since the COVID-19 pandemic was so recent, I would like to have explored the whole situation and how data privacy and patient safety were affected five to ten years in the future. I would have liked to get further data regarding the use of the U.S. COVIDWise app instead of the Australian one. Although they work fundamentally the same and the precision numbers should be very similar, the claims regarding the effects are weaker than if a case study had been performed in the U.S.

I believe that this research was extremely valuable in understanding the complexities behind the responsibility for healthcare, HIPAA, and engineer responsibility of the effects. I will use this research to assure that any future work that I may perform in the industry is reflective of the necessary ethics codes, even if there is an easier solution that would put people at risk.

Conclusion

From observing the case studies with the ISTA framework, the most important takeaways are that the legislative state of emergency and EUA declarations created additional safety and privacy concerns for healthcare workers and patients. It is impossible to overlook some of the risks from fast implementation and the possible effects that it can have on the socio-technical groups of actors in the medical network. However, it would be wrong to ignore the legislative decisions that allowed for them to happen. While the large-scale medical data remains handled from outside the realm of HIPAA's jurisdiction, it will remain to put Americans and their sensitive data at risk. To solve this, both engineers for this technology and the U.S. government need to work together to mitigate the safety and privacy concerns that were caused by the technology created and implemented during the COVID-19 era and tighten down regulations in the future.

References

U.S. Department of Labor. 2020. “Families First Coronavirus Response Act: Employee Paid Leave Rights | U.S. Department of Labor.” Retrieved March 20, 2022 (https://www.dol.gov/agencies/whd/pandemic/ffcra-employee-paid-leave).

Auxier, B., & Rainie, L. (2020, August 17). Key takeaways on Americans' views about privacy, surveillance and data-sharing. Retrieved October 31, 2021, from https://www.pewresearch.org/fact-tank/2019/11/15/key-takeaways-on-americans-views-about-privacy-surveillance-and-data-sharing/

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2020, August 17). Americans and privacy: Concerned, confused and feeling lack of control over their personal information. Retrieved November 01, 2021, from https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Brumen, Bostjan, Marjan Heričko, Andrej Sevčnikar, Jernej Završnik, and Marko Hölbl. 2013. “Outsourcing Medical Data Analyses: Can Technology Overcome Legal, Privacy, and Confidentiality Issues?” *Journal of Medical Internet Research* 15(12). doi: 10.2196/jmir.2471.

Dickler, Jessica. 2022. “Wages Are Rising but Many Americans Still Live Paycheck to Paycheck.” Retrieved March 20, 2022 (https://www.cnbc.com/2022/02/17/wages-are-rising-but-many-americans-still-live-paycheck-to-paycheck.html).

Gerke, S., Shachar, C., Chai, P., & Cohen, I. (2020, August 07). Regulatory, safety, and privacy concerns of home monitoring technologies during COVID-19. Retrieved October 17, 2021, from https://www.nature.com/articles/s41591-020-0994-1

Graham, C. M. (2020, August). Fear of the unknown with healthcare IoT devices: An exploratory study. Retrieved November 1, 2021, from https://www.researchgate.net/profile/C-Graham/publication/343861769_Fear_of_the_unknown_with_healthcare_IoT_devices_An_exploratory_study/links/5f4566c5458515b729531707/Fear-of-the-unknown-with-healthcare-IoT-devices-An-exploratory-study.pdf

Harrison, M. I., Koppel, R., & Bar-Lev, S. (2007). Unintended Consequences of Information Technologies in Health Care - An Interactive Sociotechnical Analysis. Retrieved October 17, 2021, from https://collab.its.virginia.edu/access/content/group/c117d214-ad99-469c-b01e-a46d7ff324ce/Course%20Readings/Harrison_etal_2007.pdf

Kowalska, E., Nou, A. A., Sjolinder, M., & Scandurra, I. (2016, June 21). Socio-technical challenges in Implementation of Monitoring Technologies in Elderly Care. Retrieved October 18, 2021, from https://link.springer.com/chapter/10.1007/978-3-319-39949-2_5

Latour, B. (1992). Where Are the Missing masses? The Sociology of a Few Mundane Artifacts. Retrieved October 17, 2021, from https://collab.its.virginia.edu/access/content/group/c117d214-ad99-469c-b01e-a46d7ff324ce/Course%20Readings/Latour_1992.pdf

McWilliams, A. (2017, July). Health self-monitoring: Technologies and Global Markets. Retrieved November 02, 2021, from https://www.bccresearch.com/market-research/healthcare/health-self-monitoring-technologies-markets-report.html

Murdoch, Blake. 2021. "Privacy and Artificial Intelligence: Challenges for Protecting Health Information in a New Era." *BMC Medical Ethics* 22(1):122. doi: 10.1186/s12910-021-00687-3.

Sanchez, Victoria. 2020. "Virginia's COVIDWISE App Notifies up to 120 People a Day of Possible Coronavirus Exposure | WJLA." Retrieved March 20, 2022 (https://wjla.com/news/local/virginias-covidwise-app-notifies-up-to-120-people-a-day-of-possible-exposure).

Snell, Elizabeth. 2017. "HIPAA Data Breaches, Cyber Attacks Reported by 47% of Orgs." Retrieved March 20, 2022 (https://healthitsecurity.com/news/hipaa-data-breaches-cyber-attacks-reported-by-47-of-orgs).

Snell, Elizabeth. 2018. "Hospital Data Breaches Most Common, Affect the Most Patients." Retrieved March 20, 2022 (https://healthitsecurity.com/news/hospital-data-breaches-most-common-affect-the-most-patients).

Vogt, Florian, Bridget Haire, Linda Selvey, Anthea L. Katelaris, and John Kaldor. 2022. "Effectiveness Evaluation of Digital Contact Tracing for COVID-19 in New South Wales, Australia." *The Lancet Public Health* 7(3):e250–58. doi: 10.1016/S2468-2667(22)00010-X.

Yassein, M., Hmeidi, I., Shatnawi, F., Mardini, W., & Khamayseh, Y. (2019, November 21). Smart Home is not smart enough to protect you - protocols, challenges and open issues. Retrieved October 18, 2021, from https://www.sciencedirect.com/science/article/pii/S1877050919316680