 doi:10.20944/preprints202105.0026.v1

Review

Ethical issues concerning the use of data from commercially available wearable sensors in children.

Andrie G. Panayiotou [1], Evangelos D. Protopapadakis [2*]

[1] Cardiovascular Epidemiology and Genetics Laboratory, Cyprus International Institute for Environmental and Public Health, Cyprus University of Technology and Cyprus Unit of the International Network of the UNESCO Chair in Bioethics (Haifa), Limassol, Cyprus; andrie.panayiotou@cut.ac.cy

[2] Applied Philosophy Research Laboratory, Department of Philosophy, National and Kapodistrian University of Athens, and Greek Unit of the International Network of the UNESCO Chair in Bioethics (Haifa), Athens, Greece; eprotopa@philosophy.uoa.gr

* Correspondence: eprotopa@philosophy.uoa.gr; Tel.: +302107277574

Abstract: Wearable and mobile technology has advanced in leaps and bounds in the last decade with technological advances creating a role from enhancing healthy living to monitoring and treating disease. However, the discussion about the ethical use of such commercial technology, especially in minors, is lacking behind. In this paper, we will try and summarize the ethical issues arising from the usage of commercially available wearable technology in children, highlighting issues around the consent process, mitigation of risk and potential confidentiality and privacy issues, as well as the potential for therapeutic misconceptions when used in children with chronic conditions. The above will be additionally highlighted through a relevant thought experiment.

Keywords: wearable devices; ethics; children; privacy; large data

1. Introduction

Wearable sensor-based technology has now become an integral part of everyday life aiming to help both monitor and improve one's health. These devices can use at minimum global positioning systems (GPS) and accelerometry to provide data on location and physical activity, with additional health data such as heart rate and sleep quality becoming increasingly available commercially; a recent review of relevant datasets counted up to 362 commercially available sensor-based wearable devices [1]. Research into the use of such technology has also advanced rapidly in the past decade, with publications related to "wearable devices AND sensors AND health" demonstrating a geometrical increase between 2010 and 2020 (10 publications vs >300 publications in Scopus respectively). The extended use of such devices and the amount of personal data collected, have given rise to ethical concerns, however the discussion about potential ethical issues surrounding their use has been lacking behind the relevant technological advances, especially in the case of minors, who are increasingly starting to use such devices.

Use of such devices for research purposes and ethical concerns and suggestions have been discussed before [2, 3] and are not the focus of this paper. We will review and discuss the use of such, commercially available, devices by minors, with a focus on the ethical aspects arising from such use; and more specifically the consent process, mitigation of risk and potential confidentiality and privacy issues, as well as the potential for therapeutic misconceptions when used in children with chronic conditions. The above will be additionally highlighted through a relevant thought experiment.

2. Ethical issues in use of wearable devices

Informed Consent

 doi:10.20944/preprints202105.0026.v1

Informed consent is not restricted to the use of data in research but rather is pertinent to any circumstance where personal and/or sensitive data are collected. It is both an ethical and a legal requirement especially under the current European GDPR regulation. However, the consent documents for wearable devices and their corresponding mobile or web applications are still very lengthy and more often than not, include terminology or context that is not easily understood by everyone. As a result, most consumers do not read terms of agreement or privacy policies, which leads to the routinization of consent, where the act of agreeing to the use of a technology becomes unreflective and uninformed [4]. An additional limitation is the availability of such information on the user's native language, which further hinders the "informed" part of the consent process. A very recent study demonstrated in an experimental survey using a fictitious social networking service, that 74% of participants skipped the privacy policy altogether, whereas 97% and 93% agreed to the privacy policy and terms of service respectively, without reading them. The authors report information overload as a significant negative predictor of reading the terms of service, with serious possible implications, as demonstrated by the fact that 98% missed the included clause about data sharing with the NSA and employers and giving their first-born as payment for service [5]. Such findings highlight the issues of consent in commercial settings as well as potential implications from accepting all terms and conditions without actually reading or understanding them, even more so when consent is given on behalf of a minor and even further information on additional permissions/set ups/verifications is needed. In the case of devices that are targeted directly to minors, a second consent option by the wearer –especially in the case of adolescents- might be pertinent. Whether relevant applications even require age verification for use, or the means by which they verify age has been discussed by Pasquale et al., reporting that at least in the case of social media applications many of them do not provide robust mechanisms for age verification [6].

Further, it can be easily forgotten by consumers that continual data collection is occurring and periodic re-consenting may be necessary with the use of sensor technology, as has been suggested for the use of wearable devices for research purposes [3]. In the case of minors, where parents/guardians are required to provide consent, it is even more imperative that both the type of data and the amount of data is explicitly explained as well as issues pertaining to data ownership and third-party usage, as discussed further below. If such data are to be transferred to the user's physician for example as a way of monitoring health issues, then the process should be clearly described and consent provided for each individual use of the data with clear opt-in options, whereby opting-out form a specific use should by no means make the service completely unavailable, as is the case with "blanket" consent.

Confidentiality and loss of privacy

As users of wearable devices become increasingly aware of data-ownership the pressure –and rightly so- is on the manufacturers to clarify secondary and third-party use of data. Data usage should therefore include the option of using such a device without the need to go through a cloud-based storage service, by allowing to opt-out from such services and access the data directly. The introduction of the GDPR in Europe and the HIPAA regulations provide an enforcement tool for the obligation that manufacturers have in clarifying both the type and amount of data collected by the device, but also its use. However, it is important to note that different legislations and regulations apply to various countries, with several devices allowing for transfer of data between parties that are legally bound by a different set of regulations. One example is the US HIPAA Privacy rules (https://www.hhs.gov/hipaa/for-professionals/privacy/index.html) for sensitive

 doi:10.20944/preprints202105.0026.v1

mobile Health (mHealth) data that do not apply to wearable devices as they are directly bought by consumers and not prescribed by a doctor. Furthermore, commonly collected physiological health and derived parameters, such as number of steps and heart rate, are not considered to be personal health information [7], although data collected form minors are further regulated under the Children's Data Protection Act (COPPA) in the USA.

With the ever increasing number of people, including minors, using wearable sensor-based technology, the potential for research-based use of such commercially derived data is tremendous. Whereas research studies are faced with limitations in participant numbers, time of follow-up and generalizability, real world evidence (RWE) can help researchers' access to large and generalizable population cohorts in order to be able to look at specific behavioural patterns and outcomes. This is especially important for minors as they are generally underrepresented in research. This potential for research use of real world data from commercial sources, however has to be regulated following an open and public discussion about the use and accessibility of such data, highlighting the need to preserve the user's autonomy while ensuring their safety. It is also imperative that we include minors in this discussion as they are the end-user and more often than not may have a better grasp of the technology than their parents, i.e. the person giving consent on their behalf.

Following the concept of citizen science, ownership of wearable-based sensor data obtained outside of the framework of research studies require a regulatory approach where the data remain with the user, and technical solutions are provided to allow the user to opt-out, or even better opt-in, of any reuse proposed to them. Linked with this approach, calls of public sponsors for new sensor-based data platforms for real world evidence collection may ask a regulated access by a formal procedure to speed the validation process, as has been suggested previously for the potential use of such data on cognitive performance research in a similarly vulnerable population of people with cognitive decline and Alzheimer's disease [8].

In order, however, to both inform the discussion about data ownership and privacy and enable safe usage for research, it is important, to understand how consumers feel about their data. One study on home and wearable sensors concluded that when data pertained more to their person (wearable sensors) rather than to their home (home sensors), people were more cautious and such data could trigger anxiety about their health status or overall wellbeing, while overall participants stressed the need to control the interpretation and flow of their own data [9]. This could be even more important in the case of data from user's who are minors as parents are more concerned about the information collected from their children [10]. A recent study on the perceived risks and willingness to participate in environmental health studies with personal exposure data from the USA reported that in contrast to their own data, the women asked preferred a more controlled access for their children's data. They were additionally more reluctant to share location or participate if the study involved electronic medical records, expressing concerns about privacy [11]. In a qualitative study looking at both children's and parent's perceptions about online commercial data practices, authors report that children often do not have a full understanding of how data collection practices work, although showing a degree of privacy consciousness, i.e. distinction between identifiable and non-identifiable data. They were however positive towards use of personal data in contrast to their parents [10]. What's further interesting is the reported adoption of protected measures from parents for explicit data requests but not for implicitly collected data, such as with the use of cookies or in the case of wearable devices GPS location, with some reporting a sense of lack control.

However, as mentioned above, when using commercially available sensors the consent process is more likely to be a routine process, with most users not even reading the terms and conditions [5], which makes the need for improving the consent process and making it more explicit and transparent, even more imperative.

Concerns are also usually raised regarding potential data breaches. Although data breaches are rare, they do happen and when they do they can both cause harm to the user and corrode the public's trust in the technology. There have been instances of anonymized spatial data being shared from commercial devices and applications that had the potential to identify sensitive locations and user habits [12]. Such data can be used to reveal spatial and mobility data of minors and other vulnerable groups, as well as to reconstruct social networks in adults and children and users themselves tend to consider them as "private"[13]. Major breaches of individuals' privacy with social media tools such as Facebook have occurred in the past, and citizens are rightfully worried about the use of their data [14], especially in the case of data from children. To mitigate and minimize such risks, manufacturers must exercise all available technological measures and the process regulated by data protection legislation.

Therapeutic misconceptions

Wearable devices with sensor technology are advertised as tools to help individuals monitor and improve their health and health-related behavior. Most of these devices are classified as FDA-cleared class I or II, which need much lower standards of evaluation than FDA-class III medical devices and as such their safety and effectiveness claims may not have been evaluated appropriately [15]. A review on the effectiveness of behavior change applications associated with such devices, reported that only 6 out of 23 were developed based on a theoretical model of behavioural change and that those that were theory-based were more effective in influencing outcome [16]. This is again problematic in devices targeted towards children, as these are even less-likely to be theory-based.

3. Results

A though experiment for the use of a wearable sensor-based device in children

Consider the case of John, a 12-year old perfectly healthy boy – in every other aspect, save for that John is obese: his body mass index exceeds 35, which measured against the cohort of average children of John's age places him at the 99th percentile and gives his parents a good reason to worry. Their concern dramatically increases since both John's father and mother have a quite alarming family history of type 2 diabetes and essential hypertension, respectively. Given that children in John's age are usually either reluctant or unable to commit to a healthy lifestyle, that is, be physically active and adopt a healthy diet, John's parents, after having discussed their options with John thoroughly, decided that John should be equipped with a wearable device that will track his position on a permanent basis, while at the same time it would also monitor John's blood pressure and levels of physical activity; all these data would be constantly available to John through a specialized application in his smartphone, and also reported to his parents on a real time basis, so as they may take action in case anything happens.

John's parents hope that thus John will be motivated to become more physically active, more concerned about his physical condition, and more committed to a proper dietary schedule. John on the other hand feels a lot safer since his condition will be constantly monitored not only by himself, but also by his parents, and also hopes that the device will help him lose weight soon, so as to be able to participate in activities and be much

 doi:10.20944/preprints202105.0026.v1

more acceptable by his peers, therefore, very much like his parents, he is eager to consent. Bilaterally felt satisfaction, however, doesn't suffice on its own to make any decision ethically unproblematic, especially when the autonomy and the rights of the moral agent are at stake.

a. Informed consent by minors

The use of wearable tracking and monitoring devices in minors normally give raise to autonomy-related ethical issues and concerns, since minors are generally considered not to be in the position to provide informed consent, at least not to the extent or the degree any normal adult agent typically is. To start with, as we have stated above, a 12-year-old boy can hardly be expected to fully grasp what he needs to consent to, since this is normally already difficult for grownups when it comes to reading and understanding the terms and conditions that are typically listed in consent documents. But concerns as such fuel the less controversial part of the debate, that that could easily be resolved: it would suffice if wearable devices that are equally available to minors without parental consent came with consent documents that would be easily comprehensible by minors. To the extent that this doesn't apply, however, entertaining consent-related concerns in the case of minors is perfectly justified.

Consenting to data collection and sharing also gives raise to ethical concerns when it comes to minors, and this because it requires technical and legal knowledge that is usually neither available to nor comprehensible by children of John's age. Next to this, safeguarding the security, anonymity and irrevocability of personal data related to one's health condition, lifestyle or habits is especially crucial in the case of minors such as John, since in case of failure data as such will normally accompany any minor for much longer like a shadow, and potentially affect one's chances in life or one's place in the world. In our view sensitive personal data, health-related data included, become even more sensitive in the case of minors, since they are much more vulnerable to any breach. This makes it even more imperative to secure informed consent on behalf of minors regarding the future use of data such as the ones that may be collected in John's case.

Our view, therefore, is that it is urgent to render the inclusion of minor-friendly consent documents mandatory for wearable devices that are either exclusively, or equally intended for minors. Insofar as such regulations are not implemented, however, acquiring informed consent from minors may only be contingent.

b. Living in the spotlight

A much more profound moral concern is related to the psychological impact the constant monitoring of one's physical condition and activity is expected to have on minors of John's age. Next to all the benefits that come along for John with the use of a monitoring wearable device, and regardless of the degree John's physical condition makes the use of such a device necessary or just potentially beneficial, in a sense John will be not leading a perfectly ordinary life, at least not as ordinary as that of most children of his age: John would be susceptible to develop an introspective outlook on himself, one that is neither usual nor even desirable for children of this age. Unlike other children, in a way John will be living in the spotlight not only of others, that is, his parents, but also – and most importantly – of himself. This may have certain effects on John's psychology, traits and character, that in some cases might even overweight the anticipated benefits on John's physical health: John might develop a tendency towards hypochondria, overdependence on or even addiction to his intelligent wearable device [17], introspection,

 doi:10.20944/preprints202105.0026.v1

experience a sense of autonomy loss [18]; he may become reserved and lose the spontaneity that is typical in his age, even become an egoist. In a nutshell, the use of the wearable sensor-based device may result in John experiencing a certain degree of disproportionate psychological harm, which, of course, John was not able to foresee, and has never provided his consent to – and neither have his parents.

In the face of concerns as such, the use of health monitoring devices in minors should be backed up with conclusive evidence from further psychological research; our search for relevant literature produced very poor results that mostly focus on short-term effects such as obtrusiveness and anxiety [19], and this only with regard to the general population, but not children in particular. In any case, and until such evidence has been made available, we believe that the inclusion of short, comprehensive statements on the suggested use by minors and the potential perils for one's psychological constitution and development would be a remedy against potential negative effects on underage children's mental health.

c. Privacy and the right to an open future

Health monitoring devices that are equipped with tracking sensors and report one's location on a constant basis may be a huge reassurance for parents and kids alike on the one hand, especially in cases such as John's, but they are also a radical breach in the minor's privacy: John's parents will be aware on a real time basis of John's whereabouts, while at the same time John himself would also be aware of the fact that his parents constantly are, or might be, aware of where he is and what he is doing; in a sense, John would always feel – and probably also be – under surveillance by his parents, and feel accountable to them. This, however, would severely compromise John's right to an open future, in the sense that John would be deprived of something that is normally common and typical to children of his age, that is, his privacy and its rightful offspring, the uncompromised chance to explore his own capabilities and the world.

Joel Feinberg introduced the principle of children's right to an open future to advocate the view that parents should not proceed to actions that would restrict the future options of their children, but leave them the greatest permissible scope for developing their own life choices when they reach adulthood [20]. Gradually developing into the adult John wishes and choses to be, however, requires a certain degree of privacy for him: as it normally is with most children of his age, John should have the option to decide whether he will attend or skip class, go to some poolroom or diner, drive a bike or skate to school or elsewhere, etc. In other words, John exactly like most children should have the chance from time to time to distant himself from the person he is expected to be, do silly things, in a word escape the ideal John, or even the minimally descent John. Having his activity and location monitored on a real-time basis, though, hardly leaves any place for spontaneity and nonconformity for John, and this certainly narrows down John's access to an open future. This also comes with a certain amount of injustice for John: being obese is no reason for John to be totally deprived of his privacy.

To avoid such a severe breach in minors' privacy and the consequent violation of their right to an open future it is imperative that minors should be allowed full and easily accessible opt-out options, probably also including the limited possibility of fake or coded spatial monitoring, especially for teenagers

4. Discussion

With increasing use of smart technology in everyday life it becomes imperative to discuss openly both the benefits but also potential pitfalls of such technologies, especially in the context of vulnerable groups such as children. Including the very people who use, or consent for the use, of such technologies in the discussion is deemed necessary. For one, people are more likely to use such technology if they are better informed about it and more likely to use it safely and to their benefit. One recent ethnographic study reported that people's openness to sharing data from their smart devices varied according to their individual circumstances and views about the reasons why data might be shared [9].

In light of the potential harms of privacy breaches, technology developers –much like clinical researchers- should consider the moral complexity of using tracking or sensing devices in potentially vulnerable populations (such as minors) and the possible measures they could and should take to safeguard them.

Author Contributions: AGP and EP have contributed equally to all aspects of this work.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Muzny, M., et al., Dataset of wearable sensors with possibilities for data exchange. Data in Brief, 2020. 28: p. 104978.

2. Breslin, S., M. Shareck, and D. Fuller, Research ethics for mobile sensing device use by vulnerable populations. Soc Sci Med, 2019. 232: p. 50-57.

3. Ulrich, C.M., et al., The ethics of sensor technology use in clinical research. Nursing Outlook, 2020. 68(6): p. 720-726.

4. Ploug, T. and S. Holm, Informed consent and routinisation. J Med Ethics, 2013. 39(4): p. 214-8.

5. Obar, J.A. and A. Oeldorf-Hirsch, The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services. Information, Communication & Society, 2020. 23(1): p. 128-147.

6. Pasquale, L., et al., Digital Age of Consent and Age Verification: Can They Protect Children? IEEE Software, 2020: p. 0-0.

7. Muzny, M., et al., Wearable sensors with possibilities for data exchange: Analyzing status and needs of different actors in mobile health monitoring systems. Int J Med Inform, 2020. 133: p. 104017.

8. Teipel, S., et al., Use of nonintrusive sensor-based information and communication technology for real-world evidence for clinical trials in dementia. Alzheimer's & Dementia, 2018. 14(9): p. 1216-1231.

9. Burrows, A., D. Coyle, and R. Gooberman-Hill, Privacy, boundaries and smart homes for health: An ethnographic study. Health & Place, 2018. 50: p. 112-118.

10. Desimpelaere, L., L. Hudders, and D. Van de Sompel, Children's and Parents' Perceptions of Online Commercial Data Practices: A Qualitative Study. Media and Communication, 2020. 8.

11. Udesky, J.O., et al., Perceived Risks, Benefits, and Interest in Participating in Environmental Health Studies That Share Personal Exposure Data: A U.S. Survey of Prospective Participants. Journal of Empirical Research on Human Research Ethics, 2020. 15(5): p. 425-442.

12. de Montjoye, Y.-A., et al., Unique in the Crowd: The privacy bounds of human mobility. Scientific Reports, 2013. 3(1): p. 1376.

13. de Montjoye, Y.-A., et al., On the privacy-conscientious use of mobile phone data. Scientific Data, 2018. 5(1): p. 180286.

14. Pagoto, S. and C. Nebeker, How scientists can take the lead in establishing ethical practices for social media research. Journal of the American Medical Informatics Association, 2019. 26: p. 311-313.

15. Gance-Cleveland, B., C.C. McDonald, and R.K. Walker, Use of theory to guide development and application of sensor technologies in Nursing. Nursing Outlook, 2020. 68(6): p. 698-710.

16. Zhao, J., B. Freeman, and M. Li, Can Mobile Phone Apps Influence People's Health Behavior Change? An Evidence Review. J Med Internet Res, 2016. 18(11): p. e287.

17. Mani, Z. and I. Chouk, Drivers of consumers' resistance to smart products. Journal of Marketing Management, 2017.

18. Rauschnabel, P.A., J. He, and Y.K. Ro, Antecedents to the adoption of augmented reality smart glasses: A closer look at privacy risks. Journal of Business Research, 2018. 92(C): p. 374-384.

19. Ryan, J., S. Edney, and C. Maher, Anxious or empowered? A cross-sectional study exploring how wearable activity trackers make their owners feel. BMC Psychology, 2019. 7(1): p. 42.

20. Joel, F., The Child's Right to an Open Future, in Whose Child? Children's Rights, Parental Authority, and State Power, Aiken William and LaFollette Hugh, Editors. 1980, Rowman and Littlefield: Totowa, NJ. p. 124-153.