Information Services & Use 41 (2021) 71–79
DOI 10.3233/ISU-210114
IOS Press

mHealth wearables and smartphone health tracking apps: A changing privacy landscape

Christine Suver[a,*] and Ellen Kuwana[b]
[a] *Research Governance and Ethics, Sage Bionetworks, Seattle, WA, USA*
[b] *Kuwana Consulting, Seattle, Washington, USA*

Abstract. The use of digital health technologies is changing the ways people monitor and manage their health and well-being. There is increasing interest in using wearables and smartphone health apps to collect health-related data, a domain within digital health referred to as mHealth. Wearables and health apps can continuously monitor metrics such as physical activity, sleep, and heart rate, to name a few. These mHealth data can supplement the measures taken by healthcare professionals during regular doctor's visits, with mHealth having the advantage of a much greater frequency of collection. But what are the privacy considerations with mHealth? This paper explores global data privacy protections, enumerates principles to guide regulations, discusses the tension between anonymity and data utility, and proposes ways to improve how we as a society talk about and safeguard data privacy. We include brief discussions about inadvertent or unintended consequences of digital data collection and the trade-off between privacy and public health interests, such as is illustrated by COVID-19 contract tracing apps. This paper concludes by offering suggestions for consideration about improving privacy and confidentiality notices.

Keywords: Wearables, smartphone apps, data privacy, health data, mHealth, health trackers, sociotechnical challenges, COVID-19, contact tracing

1. Introduction

Digital health is a large field that refers to the use of technology in biomedical research [1]. Popular domains of digital health include adopting electronic medical records (EMRs) or implementing telehealth and telemedicine technologies that enable remote care. mHealth is a subset of digital health that the World Health Organization defines as the "use of mobile technology to support the achievement of health objectives [2]". In a broad sense, mHealth encompasses the use of wearables, tablets, and smartphone apps that collect health-related information. mHealth is appealing to consumers, as shown by the popularity of fitness apps and wearables [3]. Mobile technologies can be set up to interact with individuals directly and prompt them to manage their health better. There is significant interest from companies and health insurance networks to harness health fitness trackers to improve employee/patient health [4,5]. Initiatives include nudges (reminders), social norms (how one compares with others), carrots (rewards), and sticks (penalties such as fees) to influence people's health-related behaviors. Physicians are also open to integrating mHealth data to inform patient care, although they largely lack the proper training to do so [6].

[*] Corresponding author: Christine Suver, Ph.D., Vice President, Research Governance and Ethics, Sage Bionetworks, 2901 Third Ave #330, Seattle, WA 98121, USA. E-mail: christine.suver@sagebase.org.

Traditionally, medical data are collected during occasional doctor visits. The patient may answer a few questions, get some tests done, and then the results get stored in their EMR. The problem with relying solely on EMR data to assess someone's health is that many people go for a healthcare checkup every year or even less often. That frequency can fail to capture the nuances in health changes that occur in people's lives. If we are to move toward personalized or precision medicine (meaning healthcare tailored to a specific individual), we need to look at up-to-date and real-life data. The patient needs to contribute frequent data, and the healthcare professional needs access to the data to inform patient care.

Technological advances make it feasible to collect new data types to provide a complete view of an individual's health. Activity trackers in wearables and health apps can record fluctuations in symptoms and quality-of-life modulators, which can be displayed daily, weekly, or monthly as numerical or graphical summaries. These trackers can directly interact with individuals, all while continuously monitoring one's physical activity, sleep, heart rate, glucose level, blood pressure, etc. [7].

Additionally, mHealth can capture data from someone's environment and track and inform their habits. For example, using the phone location to know the weather and air quality in the area or using wearable activity bands to understand the frequency and intensity of one's physical activity. This supplementary information can be integrated with routine healthcare data (e.g., blood pressure, medications prescribed) tracked through various mobile apps. The resulting rich portable data collection can supplement the EMR data collected from traditional healthcare visits.

1.1. The rapid growth of health apps shows no sign of slowing

mHealth is a growing field. Wearables and health apps are everywhere, with more than 350,000 apps available [8] and a global mHealth app market expected to reach more than $100 billion in U.S. dollars by 2023 [9]. In 2020, more than 31 million individuals used a Fitbit at least one time/week [10], and 100 million people wore an Apple watch [11]. The privacy landscape must adapt to address the wealth of data that wearables and health apps generate every second of every day. Many countries have enacted data privacy laws to regulate how information is collected, how people are informed about the storage and use of their mHealth data, and what control people have over their data once the information has been captured or shared with others [12].

2. Data protection regulations

To date, the most important data protection legislation is the European General Data Protection Regulation (GDPR) that took effect on May 25, 2018, and replaced the 1995 Data Protection Directive [13]. It is arguably the most substantial set of protections for data privacy yet. GDPR applies to twenty-eight European Union (E.U.) member states plus Iceland, Liechtenstein, and Norway. GDPR protects the personal data and privacy rights of people living in these thirty-one places and regulates the free movement of data: GDPR applies to any organization collecting personal data from these residents regardless of the organization's location. The regulation covers any processing of personal data. Under GDPR, processing data includes any of the following operations: collection, use, storage, adaptation, transmission, combination, or correction. Other countries have enacted GDPR-like privacy regulations with a few local nuances [14,15].

The U.S. does not have a comprehensive federal data privacy law. Instead, the U.S. enacted sector-specific regulations for communication, financial/credit institutions, marketing, and health information.

Some states have enacted state-specific data privacy laws such as the California Consumer Privacy Act (CCPA), Virginia Consumer Data Protection Act, or the New York Shield Act (for breach notification), but these state laws do not apply to health information. An additional fourteen states (AK, AL, AZ, CA, CO, CT, FL, IL, MA, MD, MN, NV, TX, WA) are considering adopting consumer data privacy laws. Already, privacy legislations failed or were postponed in six other states (KY, MS, ND, OK, UT, WV) [16].

In the U.S., the landmark federal regulation governing personal health data is the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule [17,18]. The Privacy Rule established for the first time a set of national standards for the protection of individually identifiable health information (called personal health identifiers, PHI). At the state level, however, additional regulations localize the implementation of HIPAA. For example, states differ about the age of majority (the age of adulthood when one is legally responsible for managing their actions and able to make decisions about their medical care) or about the HIPAA authorization expiration date (the consent to use or disclose personal health information for a purpose otherwise not permitted under the HIPAA Privacy Rule) [19]. Another example is the Experimental Research Subject's Bill of Rights mandated by the state of California for anyone participating in medical research [20].

3. Re-identification of personal data

Personal data covers many data types such as cultural, social, financial, religious, political, etc. Health data are a special category of personal data that includes sensitive information and requires even more protection. Per GDPR, personal data include any information that can be used to identify a person directly - or indirectly - through linkage. Therefore, GDPR applies to identifiable data and to de-identified or coded data stripped of direct identifiers such as a person's name or contact information. Beyond de-identification that simply obscures someone's identity, data can be anonymized, which results in data that cannot ever be used to identify a person. That is, anonymity is irreversible. Data privacy laws (data protection regulations) do not apply to anonymized data. Attempting to anonymize data is virtually impossible, however, in our society where so much personal data is publicly available. Therefore, health researchers most often collect and analyze de-identified data that are regulated by privacy laws.

Degree and type of de-identification are not equivalent. HIPAA recognizes two methods for data to be de-identified: either the Safe Harbor method (rule-based) that removes eighteen types of identifiers or the Expert Determination approach (risk-based) that involves a formal determination by a qualified expert [21]. There is no Safe Harbor equivalent under GDPR; de-identification consists of using pseudonyms or codes to mask personal identifiers. Risk-based methods must determine the risk of re-identification. These methods are contextual and should consider any possible data linkage and any likely method to perform re-identification. Adding complexity, under GDPR, the risk of re-identification must be evaluated at the time of processing, not at the time of data collection, which forces constant reassessment as data are added to the data set or analyses evolve.

4. Global privacy principles to guide regulations

Reconciling the various data privacy laws is complicated and slows international scientific collaborations that are essential to address biomedical challenges. Nevertheless, eight global privacy principles guide the development of health data privacy regulations. The collection, use, and processing of personal health data should at a minimum be:

- **Lawful**: obtained by lawful and fair means, with consent where appropriate.
- **Purposeful**: relevant and necessary.
- **Limited**: limited in scope and time and proportionate to its purpose.
- **Quality**: complete, accurate, and kept up-to-date.
- **Secure**: protected against risks of loss or unauthorized access.
- **Used as intended only**: parameters of use clearly articulated and followed.
- **Transparent**: documented and justified.
- **Controllable**: enforceable principles.

These principles were reaffirmed by WHO's statement (issued in the context of the COVID-19 pandemic) on the use and processing of health data for balancing data protection and privacy [22].

Organizations such as the Global Alliance for Genomics and Health (GA4GH, https://www.ga4gh.org/) [23] and BBMRI-ERIC (https://www.bbmri-eric.eu/ - Biobanking and BioMolecular resources Research Infrastructure, European Research Infrastructure Consortium) are working to provide practical methods to achieve compliance with privacy laws. BBMRI-ERIC has been drafting a comprehensive Code of Conduct for Health Research [24]; the release date for this guidance, however, is not yet known.

5. Regulation of health app data

More broadly, privacy laws regulate the use of personal data, which is information about an identifiable individual. What about data from wearables/smartwatches and smartphones? Are data collected through a health app considered personal data or PHI and thus regulated by privacy laws? The answer - it depends. In the U.S., apps that monitor health metrics are not regulated under HIPAA unless they are used in a regulated research context or used to make health-related decisions. The FDA does not monitor or regulate so-called "lifestyle" apps that track diet, exercise, stress levels, nutrition, sleep, or mood - even when these apps target children, as is the case for 7-Minute Workout for Kids, Cosmic Kids Yoga, and Smash Your Food, to name a few [25]. Yet health apps are increasingly handling sensitive data about users and bystanders. Think of apps related to pregnancy; apps managing prescriptions records; and apps about depression, suicidal ideation, and anxiety. These apps can collect large amounts of personal data provided by users responding to in-app questionnaires. Apps can also collect data that the user doesn't even know that they are providing.

6. Accidental or unintended consequences of data collection

Even when an app collects anonymized data, the data collection process itself can sometimes reveal a significant amount of information. One example is from Strava (see: https://www.strava.com), a health-tracking app that produces a public global heat map (data visualization that shows the magnitude of a phenomenon as color in two dimensions) of its users' exercise routes. While the purpose of the app is to reveal new exercise routes for its users, in 2018, it became clear that the mapping of soldiers' running routes in military bases gave up strategic information about the bases' locations and positions of buildings that were supposed to be secret [26].

6.1. Passive data collection

Apps and wearables are full of sensors that can provide copious amounts of information about someone, with or without individual intervention or intention. Device sensors can capture not only distances, movements, and location, but also images and sounds. The Amazon Halo band that became available in 2020 is one such wearable that listens to its user's voice, analyzes the voice tone through its artificial intelligence software, and informs users how they might sound to others [27]. These data collections are lawful and legitimate based on individuals 1) accepting the app's privacy policies and terms of service (also called terms of use or terms and conditions) and 2) opting into the sensor-based data collection necessary to use the app.

6.2. COVID-19 and contact tracing apps

During a pandemic such as COVID-19, there is a difficult trade-off between protecting someone's privacy and the public health interest, as illustrated by the utility of symptom reporting contact-tracing apps. While it may be necessary to forgo some privacy for the public good, the nature and amount of personal data collected by many COVID-related apps should give one pause. One systematic analysis looked at nearly five hundred apps related to COVID-19 in Apple iOS stores in ninety-eight countries to understand the reach and impact of the recent flurry of state-sponsored and privately developed apps for contact tracing. The analysis revealed the pervasive collection of data by COVID-related apps. Specifically: 43% ask for tracking location to be on at all times, 44% ask for access to the phone camera, 22% ask for access to phone microphone, 32% ask for access to photos, and 11% ask for access to contacts [28].

But why would contact tracing apps need access to your phone microphone or your photos? Do these apps need access to one's microphone or personal photos to track COVID-19 symptoms or alert you that you were near someone who has tested positive for COVID-19? Users might be required to agree to these broad terms and conditions to use the app features they are interested in, but most often users do not carefully review the terms and conditions to fully understand that they have granted this level of access to information on their mobile device.

7. Privacy policies and terms of service

How do we solve the privacy dilemma? How can we unlock the value of mHealth data while maintaining data privacy? The solution, certainly, is not going to be a one-size-fits-all solution. While anonymized data solve some privacy issues, there will always be a need for data with PHI: there are times when researchers need to collect identifiable data. To move us toward personalized/precision medicine, we need to collect real-life data. We will need to integrate data from a person's health history, genetics, environment, and lifestyle habits if we want to move from trial-and-error medicine to evidence-based health care tailored to a specific, unique individual. In other words, we will need to collect a lot of data - and the more data we collect, the easier it is to learn someone's identity even if the data does not include someone's name or other direct identifier. Furthermore, sharing data with PHI for research is essential, as collaboration can accelerate research progress, and it is especially beneficial for facilitating research progress on rare diseases that is slower due to the scarcity of research participants and their data.

Data may need to be anonymized, de-identified, or fully identifiable depending on its intended use. Correspondingly, we will need zones of openness, zones of privacy, and experimental zones that are mixed.

A unanimous recommendation is to inform people about the limits to anonymity and the methods and degree of de-identification. Lawful and legitimate data collection through wearable technology and health apps based on consent relies on people accepting privacy policies and terms of service - but when was the last time anyone actually read the small print?

7.1. Issues with the small print

An assessment of the terms of services of fourteen popular apps revealed that terms of service agreements are written at a 10th-grade reading level up to college level. So not everyone can read them easily or completely understand the text. Moreover, they are so lengthy as to take from ten to sixty minutes to read based on an average adult reading speed. Someone in the U.S. would need to devote close to two hundred and fifty hours to complete reading all of the fine print associated with the online services an average person uses [29].

Privacy policies are similarly written. Over time, they have become longer and more complex. The privacy policy for Google in 1999 was six hundred and ten words; by 2018, it was two thousand seven hundred and twenty two words. In 2019, after GDPR, it had reached four thousand and thirty-six words, which represents a six-fold increase in length over the twenty-year span [30]. At an average reading speed of approximately three hundred words per minute, an adult would need at least twenty minutes to read a single privacy policy. If you had thirty apps on your phone, it would take you more than ten hours to read all the privacy policies. When GDPR was implemented, every website and app updated its privacy policy, and it would be reasonable to guess that no company shortened or simplified theirs. As *The New York Times* Privacy project concluded, privacy policies are an "incomprehensible disaster [31]."

7.2. Parallels with informed consent process

The same way we have worked to improve the informed consent process for mobile-mediated research over the past six years [32], we must similarly work to better explain data protections and privacy while simultaneously satisfying any existing regulatory requirements that govern mHealth data. Additionally, any entity that collects health data needs to communicate the concept of data privacy and the impact of collecting complex data sets in a clear and accessible manner to the general public. Research supports that people better understand complicated concepts when concepts are presented in chunks of information instead of all at once [33] - framing data privacy as a set of conversations rather than one be-all-end-all form is a step in the right direction. Those who conduct clinical research prefer informed consent to consist of a series of conversations about a research study, then an interactive review and signing of the consent form (i.e., an informed consent *process*) rather than simply and only signing the consent form (i.e., a single document with little to no discussion) [34].

7.3. Real-world examples of simplified privacy policies

There are some intriguing examples of companies trying to improve their communications related to informing users about data use and privacy policies. Strava issued a new privacy policy effective December 15, 2020 that introduced a "privacy label." Like a food label on a grocery store item, Strava's privacy label is easy to read and understand - and is short [35]. Also noteworthy is Apple's privacy label: as of December 14, 2020, developers must self-report the information they collect [36]. While these efforts are still too tepid, they are a step in the right direction and an improvement in informing people.

Drawing on extensive work that we have conducted and from best practices in the informed consent process for research participants, we developed a resource we call the Privacy Toolkit for Mobile Health Research Studies. The toolkit provides biomedical researchers with a catalog of design tools and patterns to create robust resources about data privacy and data management that research participants can refer to during an mHealth study. The Privacy Toolkit promotes ongoing discussion with research participants, creating opportunities for users to be reminded about the mHealth data they contribute and reaffirm their agreement with the researchers' data collection and data handling plans [37].

8. Conclusion

Protecting privacy in the age of big data is challenging. We need robust governance mechanisms that enable data sharing for scientific research, but protect individuals who are contributing information - sometimes sensitive or personal information - against violations to their privacy. To achieve this tricky balance, there is no one-size-fits-all solution. One prospect is a more nuanced approach with different data privacy zones akin to camera privacy zones that can hide a field of view. Privacy zones for data are a better solution because they let people determine what level of data privacy they want for any given information about themselves at any given time. Lastly, engaging research participants and regulatory bodies that govern research, such as institutional review boards, is essential if we are to realize the promises of biomedical research while also addressing concerns and safeguarding individual's privacy rights.

About the authors

Christine Suver (corresponding author) leads the Research Governance and Ethics group at Sage Bionetworks. The group develops and pilots data sharing models and tools to enable open research collaborations. In her work, she helps research participants and researchers determine the appropriate governance approach to contribute, collect, access, and share research data responsibly.

It starts with research participants. She designs eConsent experiences to better inform participants about the risks and benefits of participating in research. She explains the real-world implication of big data analysis, comprehensive data linkage, and the impact on their privacy. Christine is particularly interested in developing new eConsent to support the autonomous decision of populations with a wide range of memory and cognitive ability.

She also helps researchers determine the governance conditions that enable them to work collaboratively and comply with ethical and regulatory requirements. Christine co-chairs the Governance Working Group of the (exceptional) National COVID Cohort Collaborative initiative (N3C), to enable dozens of institutions to responsibly share clinical data for urgent COVID-related research. E-mail: Christine.suver@sagebase.org; Phone: (206)-928-8242. ORCID: https://orcid.org/0000-0002-2986-385X.

Ellen Kuwana is a trained scientist (MS in neuroscience from University of California San Francisco) with more than ten years of basic, clinical, and translational research experience. Her areas of subject matter expertise include neuroscience, molecular biology, cancer biology, and bioethics. She is also the Founder of WeGotThisSeattle, a COVID-19 relief project that coordinated food to more than 46,000 frontline workers during the pandemic. ORCID: https://orcid.org/0000-0002-7092-5434; LinkedIn: https://www.linkedin.com/in/ellenkuwana/.

References

[1] Center for Devices and Radiological Health, What is digital health? 2020. [Online]. Available: https://www.fda.gov/medical-devices/digital-health-center-excellence/what-digital-health, accessed July 11, 2021.

[2] World Health Organization. *MHealth: New Horizons for Health Through Mobile Technologies,* World Health Organization, 2011, [Online]. Available: https://www.who.int/goe/publications/goe_mhealth_web.pdf, accessed July 11, 2021.

[3] J. McCarthy, One in five U.S. adults use health apps, wearable trackers, *Gallup*, 11-Dec-2019. [Online]. Available: https://news.gallup.com/poll/269096/one-five-adults-health-apps-wearable-trackers.aspx, accessed July 11, 2021.

[4] With fitness trackers in the workplace, bosses can monitor your every step - and possibly more, *The Washington Post,* 15-Feb-2019 [Online]. Available: https://www.washingtonpost.com/business/economy/with-fitness-trackers-in-the-workplace-bosses-can-monitor-your-every-step–and-possibly-more/2019/02/15/75ee0848-2a45-11e9-b011-d8500644dc98_story.html, accessed July 11, 2021.

[5] D. Soliño-Fernandez, A. Ding, E. Bayro-Kaiser and E.L. Ding, Willingness to adopt wearable devices with behavioral and economic incentives by health insurance wellness programs: Results of a US cross-sectional survey with multiple consumer health vignettes, *BMC Public Health* **19**(1) (2019), 1649. doi:10.1186/s12889-019-7920-9. [Online], accessed July 11, 2021.

[6] Stanford Medicine, Stanford Medicine Health Trends 2020 Report 2020, https://med.stanford.edu/dean/healthtrends.html, accessed July 11, 2021.

[7] A. Henriksen et al., Using fitness trackers and smartwatches to measure physical activity in research: Analysis of consumer wrist-worn wearables, *J. Med. Internet Res.* **20**(3) (2018), e110. doi:10.2196/jmir.9157. [Online], accessed July 11, 2021.

[8] MHealth economics 2017 – current status and future trends in mobile health, 01-Nov-2017. [Online]. Available: https://research2guidance.com/product/mhealth-economics-2017-current-status-and-future-trends-in-mobile-health/, accessed July 11, 2021.

[9] IQVIA, The Growing Value of Digital Health, https://www.iqvia.com/insights/the-iqvia-institute/reports/the-growing-value-of-digital-health, accessed July 11, 2021.

[10] Fitbit revenue and usage statistics (2021), 23-Oct-2020. [Online]. Available: https://www.businessofapps.com/data/fitbit-statistics/, accessed July 11, 2021.

[11] F. Espósito, There are more than 100 million people wearing an Apple Watch, says analyst - 9to5Mac, 12-Feb-2021. [Online]. Available: https://9to5mac.com/2021/02/11/there-are-more-than-100-million-people-wearing-an-apple-watch-says-analyst/, accessed July 11, 2021.

[12] *Data Protection Around the World: Privacy Laws in Action*, E. Kiesow Cortez (ed.), 1st ed. T.M.C. Asser Press, The Hague, Netherlands, 2020, [Online]. Available: https://www.cnil.fr/en/data-protection-around-the-world, accessed July 11, 2021.

[13] GDPR Archives - GDPR.eu. [Online]. Available: https://gdpr.eu/tag/gdpr/, accessed July 11, 2021.

[14] D. Simmons, 12 countries with GDPR-like data privacy laws. [Online]. Available: https://insights.comforte.com/12-countries-with-gdpr-like-data-privacy-laws, accessed July 11, 2021.

[15] Office for Human Research Protections, International Compilation of Human Research Standards, 2020. [Online]. Available: https://www.hhs.gov/ohrp/international/compilation-human-research-standards/index.html, accessed July 11, 2021.

[16] US state comprehensive privacy law comparison. [Online]. Available: https://iapp.org/resources/article/state-comparison-table/, accessed July 11, 2021.

[17] Health Information Privacy, 26-Aug-2015. [Online]. Available: https://www.hhs.gov/hipaa/index.html, accessed July 11, 2021.

[18] A. Act, Health insurance portability and accountability act of 1996, *Public Law* **104** (1996), 191, [Online]. Available: http://www.eolusinc.com/pdf/hipaa.pdf, accessed July 11, 2021.

[19] M. Doerr, S. Grayson, S. Moore, C. Suver, J. Wilbanks and J. Wagner, Implementing a universal informed consent process for the All of Us Research Program, *Pac. Symp. Biocomput.* **24**: (2019), 427–438. doi:10.2139/ssrn.3277573. [Online]. Available: https://www.ncbi.nlm.nih.gov/pubmed/30963079, accessed July 11, 2021.

[20] Law section. [Online]. Available: https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=24172.&lawCode=HSC, accessed July 11, 2021.

[21] Office for Civil Rights (OCR), Methods for De-identification of PHI, 07-Sep-2012. [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html, accessed July 11, 2021.

[22] Joint statement on data protection and privacy in the COVID-19 response, *Neurosciences* **26**(1) (2021), 111–112, [Online]. Available: https://www.un.org/sites/un2.un.org/files/joint_statement_on_data_protection_and_privacy_in_covid-19_response.pdf, accessed July 11, 2021.

[23] GDPR brief: Codes of conduct under the GDPR: A useful but challenging tool to enable responsible international data sharing. [Online]. Available: https://www.ga4gh.org/news/gdpr-brief-codes-of-conduct-under-the-gdpr-a-useful-but-challenging-tool-to-enable-responsible-international-data-sharing/, accessed July 11, 2021.

[24] A code of conduct for health research. [Online]. Available: http://code-of-conduct-for-health-research.eu/, accessed July 11, 2021.

[25] E.A. Store, Best Health and Fitness Apps for Kids, 22-Jun-2017. [Online]. Available: https://www.educationalappstore.com/best-apps/5-apps-to-promote-a-healthy-lifestyle-to-kids, accessed July 11, 1021.

[26] J. Hsu, The Strava Heat Map and the End of Secrets: The US military is reexamining security policies after fitness tracker data shared on social media revealed bases and patrol routes, *Wired*, 29-Jan-2018. [Online]. Available: https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/, accessed July 11, 2021.

[27] I.A. Hamilton, AI experts doubt Amazon's new Halo wearable can accurately judge the emotion in your voice, and worry about the privacy risks, *Business Insider*, 29-Aug-2020. [Online]. Available: https://www.businessinsider.com/experts-skeptical-amazon-halo-judges-emotional-state-from-voice-2020-8, accessed July 11, 2021.

[28] J. Albright, The pandemic app ecosystem: Investigating 493 Covid-related iOS apps across 98 countries, *Medium*, 28-Oct-2020. [Online]. Available: https://d1gi.medium.com/the-pandemic-app-ecosystem-investigating-493-covid-related-ios-apps-across-98-countries-cdca305b99da, accessed July 11, 2021.

[29] Visualizing the length of the fine print, for 14 popular apps, *Business Insider,* https://markets.businessinsider.com/news/stocks/terms-of-service-visualizing-thelength-ofinternet-agreements-1029104238, accessed July 11, 2021.

[30] R. Sobers, The average reading level of a privacy policy, *Varonis*, 2018. [Online]. Available: https://www.varonis.com/blog/gdpr-privacy-policy/, accessed July 11, 2021.

[31] K. Litman-Navarro, We read 150 privacy policies. They were an incomprehensible disaster, *The New York Times*, 12-Jun-2019. [Online]. Available: https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html, accessed July 11, 2021.

[32] M. Doerr, C. Suver and J. Wilbanks, Developing a transparent, participant-navigated electronic informed consent for mobile-mediated research, 22-Apr-2016 [Online]. Available: https://papers.ssrn.com/abstract=2769129, accessed July 11, 2021.

[33] G.A. Miller, The magical number seven plus or minus two: Some limits on our capacity for processing information, *Psychol. Rev.* **63**(2) (1956), 81–97, [Online]. Available: https://www.ncbi.nlm.nih.gov/pubmed/13310704, accessed July 11, 2021.

[34] N.E. Kass, H.A. Taylor, J. Ali, K. Hallez and L. Chaisson, A pilot study of simple interventions to improve informed consent in clinical research: Feasibility, approach, and results, *Clin. Trials* **12**(1) (2015), 54–66. doi:10.1177/1740774514560831. [Online], accessed July 11, 2021.

[35] Strava Privacy Policy. [Online]. Available: https://www.strava.com/legal/privacy, accessed July 11, 2021.

[36] Apple Inc, App privacy details - App Store - apple developer. [Online]. Available: https://developer.apple.com/app-store/app-privacy-details/, accessed July 11, 2021.

[37] Privacy Toolkit for mobile health research studies - sage bionetworks, 21-Jun-2019. [Online]. Available: https://sagebionetworks.org/tools_resources/privacy-toolkit-for-mobile-health-research-studies/, accessed July 11, 2021.