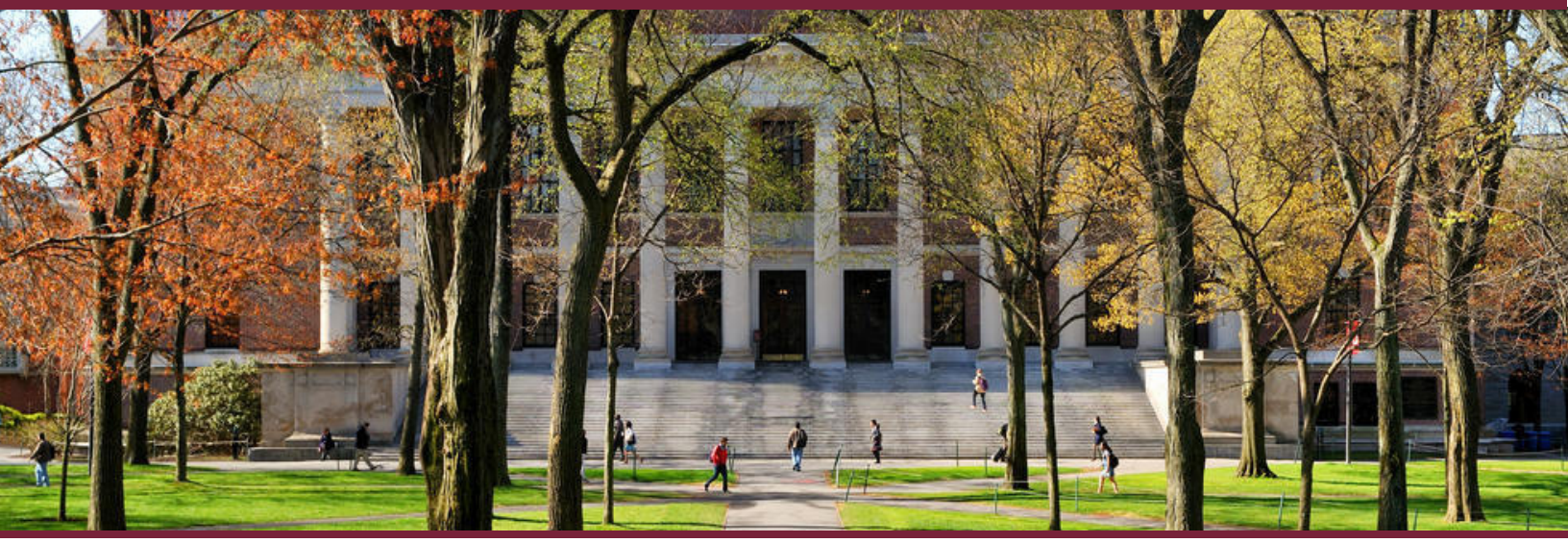
COVID-19 Rapid Response Impact Initiative | White Paper 18

Ethical Implementation of Wearables in Pandemic Response: A Call for a Paradigm Shift

May 18, 2020



Marielle S. Gross, MD, MBE[1]
Robert C. Miller[2]
Assya Pascalev, PhD [3]

EDMOND J. SAFRA Center for Ethics

Abstract

Wearable technologies, a class of information technology devices uniquely designed to be worn on an individual's body, are being implemented in the strategic response to COVID-19. Their form and function establish a unique degree of intimacy with the human body, raising a set of distinct ethical concerns related to use of the data they create, record, analyze and transfer. We discuss two paradigmatic applications of wearables in this setting: tracking persons via GPS and bluetooth and harnessing of biometric surveillance for disease management and prevention. We then highlight the nuanced ethical concerns for privacy and respect for persons, autonomy, and justice related to the design, oversight and embedded structure of wearable technology, the nature of relevant informed consent regarding use of data collected by wearable devices, and potential for these applications to exacerbate underlying disparities. Finally, we propose three prospective solutions for keeping data both decentralized and concealed and for application of Mediating Institutions of Data (MIDs) which may enable appreciation of potential benefits of wearables, both during COVID-19 specifically, and more broadly, while minimizing the ethical harms.

[1] Johns Hopkins Berman Institute of Bioethics, Bloomberg School of Public Health, Johns Hopkins University, Baltimore, Maryland, USA
[2] ConsenSys Health, New York City, New York, US
[3] Department of Philosophy and Department of Interdisciplinary Studies, Howard University, Washington, D.C., USA; and Bulgarian Center for Bioethics, Sofia, Bulgaria.

Table of Contents

01 Introduction

COVID-19 is the first pandemic to occur against the backdrop of unprecedented technological advancement, particularly of information technology. Pinpointing and tracking individual behavior and health has been an essential component of the international response to the threat of the coronavirus, and there has been a diverse array of digital tools for containing the pandemic, from contact tracing apps[4] to geolocation trackers,[5] wristbands,[6] and ankle bracelets.[7] The immense surveillance capabilities of such digital tools have the potential to help combat the spread of COVID-19. By the same token, however, these digital tools, as currently designed, deployed, and regulated, pose a threat both to the privacy of health data and to the individual's right and ability to control such data and other sensitive personal information that may be collected digitally and processed by governments, health agencies, and other stakeholders as part of the pandemic response, thus challenging the core values of autonomy and privacy.[8]

Among the rapidly growing arsenal of digital tools for health data collection, wearables represent a unique category. These are computing devices that are worn on our persons, characteristically enabling continuous data collection, transmission, recording, analysis, and, potentially, sharing. It is precisely this process of externalizing continuous information about the individual's physical body, physiological parameters, and sense of wellbeing to centralized stakeholders which presents the possibility of using wearables to address COVID-19—itself premised on transmission between individuals—but also presents the associated dangers. As contact tracing, massive upscaling of testing, and data aggregation

[4] Valentino-DeVries, Singer, and Krolik, 2020. For an overview of COVID-19 surveillance methods in different countries, see also Woodhams, 2020; Hamilton, 2020; and Smith, 2020.
[5] Cozzens, 2020.
[6] Wristband for COVID-19 tracking have been implemented in Hong Kong (see Hong Kong, 2020) and are under consideration in Liechtenstein (Khan, 2020).
[7] The use of ankle bracelets for COVID-19 quarantine enforcement was considered by the government of Hawaii and was implemented in Kentucky; see Satter, 2020.
[8] Parker et al., 2020; and OECD, 2020.

Introduction

is rolled out worldwide, the appropriate role of wearable technology in the pandemic response must be considered, particularly given the significant personal and public interests at stake, the propagation and popularity of these devices, and the pressing need for ethical solutions during ongoing waves of pandemic disease response and recovery.

In this paper, we call for a paradigm shift in how data extracted through digital surveillance tools such as wearables is collected, accessed, and processed. Such tools ought to guarantee the privacy of the data subject and give the individual full control over their personal and health-related data. To this aim, we present a range of alternatives, focusing on advanced privacy-preserving technological solutions which meet the ethical requirements of privacy and subject-centered data control, while retaining the benefits harnessed by digital technology and big data for the purposes of pandemic control.

We begin by outlining the two primary uses of wearables for COVID-19 response and review the ethical concerns raised by their applications for tracing, tracking, and biometric surveillance. We maintain that, under the currently dominant legal and technological standards, the use of wearables with their intimate connection to the human body poses a serious threat to individual freedom, autonomy, and privacy, and may lead to normalization of surveillance of one's person, which could have lasting negative effects on individual rights and democracy long after the current pandemic subsides. We further maintain that the loss of privacy is not intrinsic to such technologies and that we do not need to sacrifice individual privacy in order to reap the benefits these tools offer with respect to health data collection and analysis. We conclude by introducing a number of alternative technological solutions that meet the ethical requirements of respect for individual autonomy and data privacy and instantiate the paradigm shift towards the ethical design and use of wearables. Moreover, even though the focus of this analysis is wearables, our analysis has much broader implications and the solutions we propose could strengthen the privacy protections in all domains where personal data is collected through digital means.

02 Two Cases Illustrating Use of Wearables during COVID-19 Response

In the context of the COVID-19 response, wearables have two primary uses: They can be used for GPS location and Bluetooth tracking of persons who test positive for the virus, or they can e used to for the tracking of persons under investigation (PUI) or at-risk contacts. The location-focused wearables also function as geo-tracing devices, which, informed by collateral information sources, help to identify those who merit tracking, that is, those who need quarantine and may trigger tracking of others. Wearables can also be used for more general biometric surveillance intended to detect early signs of illness in an individual. In what follows, we consider an example of each use and outline the ethical challenges posed by it.

Tracking of Persons through GPS and Bluetooth Technology

In March 2020, the South Korean government implemented a smartphone app to supervise self-quarantine of those who met criteria for confirmed contacts with COVID-positive individuals. The purpose of the app was to enable disease surveillance, including symptom reporting, mobile testing, and, critically, GPS monitoring of location with triggered warnings for those who leave their prescribed quarantine locations. The major purpose was to prevent asymptomatic "super spreaders" from unknowingly spreading the virus. However, some asymptomatic individuals were incentivized to leave their phones at home so they could leave their quarantined location undetected. A rash of successful attempts to fool the app prompted the Korean government to implement tracing wristbands as mandatory for those under quarantine who violated restrictions. This is the paradigmatic state-sponsored use of wearables in the COVID-19 response. Much like historically implemented ankle bracelets for those under house arrest, the wristbands are designed to ensure people do not leave their phones at home and to alert authorities if removal is attempted. Other countries have since explored implementation of similar wearable devices.[9]

[9] BBC, 2020.

Biometric Surveillance

Wearables are also being used to enable broad biometric surveillance on healthy populations, as opposed to on known or suspected cases or contacts, for the purpose of early detection of infections, which would thereby prompt targeted self-isolation and testing. A salient feature of this use of wearables is that the devices are generally created for one purpose: to offer individuals insights into their health, including fitness, sleep, or fertility tracking. However, in the COVID-19 response, these same wearables are being utilized for another, very different purpose that is intended to benefit not the individual but the public and to facilitate the governmental response to the pandemic, for example, by grafting wearables into studies for early detection of COVID-19. Such a use is distinct from using an app or device specifically designed and implemented for pandemic disease tracking. Unlike the devices exclusively based on geolocation, the biometric detecting wearables are relatively high tech and embedded with a variety of sensors which have been variably vetted as capable of accurately capturing more complex biological data.

A notable example of using wearables for biometric disease surveillance is the Oura ring in the United States. Originally designed by a private company seeking to improve users' sleep by monitoring, recording, and analyzing their data related to sleep,[10] the ring has found a novel application in COVID-19 settings due to its ability to capture body temperature and heart rate. Prompted by an Oura user's report on social media that the ring alerted him of his illness before he noticed any symptoms, researchers at UCSF hypothesized that since fever is a salient early symptom of the disease, the ring may be useful in sensing early cases of COVID-19 based on elevations in temperature and associated heart rate changes.[11] At the time of the writing of this paper, several studies of the Oura ring are being implemented across a health care system to survey the vital signs of a high-risk group (health care workers) and others who volunteer to participate.[12]

[10] For a detailed description of the Oura ring, see the manufacturer's webpage: https://ouraring.com/
[11] OURA, 2020.
[12] In some, but not necessarily all cases, those participating in the study must purchase the ring.

03 Ethical Concerns

Wearables are also being used to enable broad biometric surveillance on healthy populations, as opposed to on known or suspected cases or contacts, for the purpose of early detection of infections, which would thereby prompt targeted self-isolation and testing. A salient feature of this use of wearables is that the devices are generally created for one purpose: to offer individuals insights into their health, including fitness, sleep, or fertility tracking. However, in the COVID-19 response, these same wearables are being utilized for another, very different purpose that is intended to benefit not the individual but the public and to facilitate the governmental response to the pandemic, for example, by grafting wearables into studies for early detection of COVID-19. Such a use is distinct from using an app or device specifically designed and implemented for pandemic disease tracking. Unlike the devices exclusively based on geolocation, the biometric detecting wearables are relatively high tech and embedded with a variety of sensors which have been variably vetted as capable of accurately capturing more complex biological data.

The use of wearable devices in the COVID-19 response raises ethical concerns which have not been properly analyzed and addressed.[13] The widespread collection of personal health information by way of wearables in the current pandemic has the potential to solidify the normalization of surveillance in society and may lead to mandated continuous surveillance of the human body by governments, private companies, employers, and other entities who have a stake in our data, which would have serious long-term potential to obliterate privacy, undermine moral agency, and create other risks to individual freedom and rights that stand to persist long after this particular disease threat has passed. Before we propose a set of solutions to the ethical challenges posed by wearables in pandemic response, we outline the major ethical challenges specific to this category of digital tools. Critically, these challenges,

[13] A notable exception to the current lacunae of ethical and legal analyses of the use of digital technology in pandemic response is the analysis of mobile phone apps for contract tracing by Parker et al., 2020.

Ethical Concerns

and likewise the need to implement the proposed solutions, stand whether or not wearables prove effective in combating COVID-19, as their use for pandemic response is a paradigmatic and illustrative "use case" for the ethical, legal, and social dimensions of the broader application of this technological category.

Technology Design, Oversight, and Embedded Ethical Dilemma

One set of ethical concerns related to the use of wearables in pandemic response stems from the fact that the wearable technology being harnessed for disease surveillance and response in the COVID-19 pandemic was created for radically different contexts. Specifically, the devices are almost exclusively developed by private firms that are not a part of the traditional health care system (i.e., they are not "covered entities" or business associates under HIPAA) and that have commercial interests in selling the devices themselves and/or the data the devices collect. As such, wearables are, for the most part, not subject to the same regulatory scrutiny and oversight as other medical devices and do not offer the same level of control and privacy protections individuals have come to expect with regard to their health data.

As one of us has noted elsewhere, there is a gap between the high level of protection afforded to personal health data collected and used in clinical and research contexts and the low level of protection of the same data when collected outside the clinical context through digital tools such as mobile phone apps or fitness trackers.[14] While the former is regulated by strict standards codified by HIPAA and the Common Rule in the US and the Convention on Human Rights in Biomedicine in Europe, health data collected and stored on cloud-based and internet-powered devices and platforms is subject to laws of commerce and, in the USA, are regulated by a patchwork of bodies including the Federal Trade Commission and state attorneys general. They have vendor-friendly and obscure privacy rules and proprietary claims over the personal data they collect as evidenced by their Terms of Service (ToS).

[14] Pascalev, 2018.

Ethical Concerns

Technology Design, Oversight, and Embedded Ethical Dilemma

Consequently, in almost all cases individuals who use wearables for early detection of potential infections do not have the legal protections traditionally associated with health data. This creates unprecedented structural power asymmetries between individuals and those who produce the wearables, and process and manage the associated data. Under such conditions, and without transparency and adequate oversight, the use of wearables in pandemic response could pose serious threat to individual autonomy and privacy, thereby exacerbating social and political inequality and the stigmatization of vulnerable groups. This in turn threatens to undermine democracy and freedom, though, as we intend to show, this does not have to be the case.

Challenges to Meaningful Informed Consent

Moreover, current legal frameworks and ethical oversight of opt-in or opt-out structures create undue burdens on individuals who may want to maintain their privacy.[15] Empirical and social science research has demonstrated that the current processes and format of obtaining informed consent for the use of digital tools by accepting the Terms of Use and Privacy Policies create cognitive barriers that interfere with individuals' ability to make informed, rational choices about the costs and benefits of consenting to the collection, use, and disclosure of their personal data. There are two structural issues that apply here.

First, there are issues of scale. The average person manages multiple devices and uses countless services online. Each of these has its own privacy policy and must be managed on its own. Given the sheer number of entities with which a person interacts, it is unreasonable to expect that they can manage their privacy settings separately for each entity that they engage with.[16]

[15] See Solove, 2013.

[16] A 2008 Carnegie Mellon study by Cranor and McDonald (2008) calculated that it would take the average user 76 workdays to read the Privacy Policies of the online services the user accesses.

Ethical Concerns

Challenges to Meaningful Informed Consent

This problem is compounded by a confusing legal landscape where it is difficult to tell what protections your data has in what context, and where organizations update their policies, potentially without notice. Furthermore, additional complications can arise when companies are acquired or merged with others, as consumers may not trust the new owners and the terms of use they previously agreed to may change. A salient example of this is the acquisition of FitBit by Google.[17]

Second, there are issues of aggregation. Many threats to individual privacy result not from single pieces of data but instead from the aggregation of different pieces of data collected by different entities over time. For example, you might be comfortable sharing your location data with a company for one purpose, but be uncomfortable if that location data were paired with your health data. However, the ways in which one individual's data could be shared and aggregated with another individual's data is often not known beforehand by the entity requesting the data, and if it is known, that use might change or not be disclosed to the individual whose data is in question. For example, data related to one's COVID-19 positive contacts may be repurposed for related or unrelated projects. Without knowing these uses in advance, it is impossible for individuals to properly weigh the costs and benefits of sharing data and thus to provide meaningful informed consent. Furthermore, data which may be deidentified when split may become identifiable when taken as an aggregate. This highlights the mounting challenges related to a vacuum of ethical and legal oversight for novel means of data creation and collection: the lack of clarity as to the present and future uses of the data collected by wearables and the potential for abuse.

Potential to Exacerbate Disparities and Discrimination

As with other aspects of the pandemic, there is a potential for wearable devices to impact individuals differently based on preexisting differences and disparities. This potential is uniquely fueled by the focus of

[17] Another example of this is Sanger, 2020.

Ethical Concerns

Potential to Exacerbate Disparities and Discrimination

sensors and tracking of the physical body—playing off the underlying vulnerability and differences of women and historically marginalized groups who have not received similar amounts of liberty and attention in clinical or sociological research (including the development and testing of the sensors themselves).

For example, a sensor that detects minute changes in body temperature may be very accurate when detecting a small change in the body temperature of a male individual but less so when reading temperature changes in a reproductive-aged women whose body temperature fluctuates as a function of biological processes. The consequence may be increased imposition of self-quarantine among women, if similar changes in temperature indicate similar infectious warning signs, although women's actual risk may be less accurately characterized. Over time this may disproportionately impact women's employment and compensation, potentially increasing disparities in pay gaps and job security during the COVID recovery and subsequent waves of the pandemic.

On the other hand, acknowledgement of the differences in biometric parameters, during pregnancy, for example, has led to data-analyzing organizations to seek additional information from women regarding their pregnancy status. While this is clinically justified by virtue of its impact on vital signs, pregnancy has also been used to target women for workplace discrimination and other stigmatizing treatment.

The similar process as applied to natural variations in body temperature, respirations, etc., results in eliciting additional highly sensitive health information from women in order to improve devices' performance. The lack of security of this data and its potential reappropriation and alternative uses means that data from wearables applied in this fashion creates distinct vulnerabilities for reproductive-aged women. Indeed, of the wearables being investigated for use in the COVID-19 response, a whole category includes devices originally intended to be used for monitoring monthly ovulation and fertility. Additional ethical concerns may arise when devices specifically calibrated for use in women's reproduction

Ethical Concerns

Potential to Exacerbate Disparities and Discrimination

are appropriated for broader use for general population health and the male body. In sum, the wearables may either be less accurate for women, or seek increasingly large amounts of intimate information from women and vulnerable groups, which would potentially exacerbate inequities related and unrelated to pandemic response.

As frequently discussed in the context of immunity certificates, wearables may also be used by employers as a means of tracking, verifying, and optimizing the COVID status or risk of their employees. This creates a troubling slippery slope given the multi-use nature of the data collected and the potential to normalize bodily control and monitoring outside of the COVID-19 response. The imagery of collars—the original wearables used to track and control pets and slaves—is evocative of the concerns and the discomfort that we may not fully appreciate. Moreover, wearable devices stand out for their intimate connection with the human body and their continuous collection of real-time data. As a device meant to be worn continuously, a wearable has a level of personal invasion that is higher than that of a mobile phone app, even when they are collecting the same type of data. In the US, there may already be a legal precedent for this view in the case of Carpenter v. US, in which the Supreme Court of the United States noted that data collected through GPS tracking was considered intimate thus protected under the Fourth Amendment.[18] The Court further noted that "a cell phone is almost 'a feature of human anatomy' that enables 'near perfect surveillance' as if it were attached like an 'ankle monitor" to a user, enabling an 'intimate window into a person's life,' providing the ability to track, monitor and surveil someone in a way that was never before practicable; especially for the extended periods of time routinely captured by Cell phone cell site location records."[19] It is this peculiar nature of wearable devices, with their corporality and bodily intimacy making them particularly invasive and potentially dehumanizing, that adds to the need for scrutiny and alternative solutions.

[18] Carpenter v. US, No. 16-402, 585 U.S. ____ (2018).
[19] See Carpenter v. US, No. 16-402, 585 U.S. ____, pp.12-13 (2018). We are indebted to Joel Schwarz, JD, CIPP, for this point and for providing the legal expertise and language to capture it here.

04 Alternatives and Future Directions

The ethical challenges posed by the use of wearables in pandemic response stem from the interplay of two factors: the lack of adequate legal framework and oversight, and the business model of dominant tech vendors predicated on commercial collection and trade of individual users' data, which Zuboff dubs "surveillance capitalism."[20] We maintain that the threats to user privacy are not intrinsic to digital tools but are a result of the way they were adopted and implemented in the current technical architecture and data-based business models. Rather than acquiesce to an Orwellian future that threatens our core values, in which our expectations of privacy and surveillance compromise or jettison completely our foundational human dignity, we must consider alternatives that preserve benefits without the associated risks and harms of the current framework.

There are three broad strategies—keeping data decentralized, keeping data private, mediating institutions of data—and a host of privacy-preserving technologies[21] that have potential to be employed. Note that while we discuss the theoretical merits of these strategies, there is significant work lying ahead before they could be deployed at scale in the real world. It will be critical for these technical solutions and novel approaches to privacy and individual rights to be intentionally planned and embedded into the devices and their corresponding systems' design.

Keeping Data Decentralized

The first strategy addresses the liability created by the dominant practice of centralizing data for the purposes of extracting value. The strategy to combat relevant risks to user privacy and interests requires application of privacy-preserving technology. Firstly, devices should be designed to keep data they

[20] Zuboff, 2019.
[21] Miller and Gross, 2019.

Alternatives and Future Directions

Keeping Data Decentralized

collect locally. Doing so would allow users to retain custody of their data and reduce the possibility of privacy violations by third parties. If the user's data is needed by a third party for some purpose, they should make a specific request to the user for a limited set of data needed to carry out a task. Moreover, it often is not necessary to send data to a cloud server to perform data analytics, so whenever possible, this should also be performed on devices.

For example, **federated learning** is a novel privacy-preserving technology where a network of participants can gain the benefits of traditional machine learning without requiring that data be sent to a central location to be processed in aggregate.[22] As a result, one can learn from data without the risks associated with sharing with other parties. In contrast to strategies traditionally employed, federated learning works by "sending the algorithm to the data." Instead of sending data to a central location to be processed, data is trained on local servers, and only the resulting algorithms, but not the underlying data, are shared with other parties.

This strategy is especially significant because it obviates the need to create external data stores, which, once created, often exist in perpetuity and may be breached or utilized by third parties for a variety of projects or under different terms of service. Under this model, the user maintains sole custody of their personal data, and they can allow access to take advantage of or participate in centrally mediated projects, such as COVID-19 surveillance and tracking, without creating the risk associated with the external, centralized data repositories that are outside their control. Federated learning is one promising new technology among many which decentralize data custody while still enabling data utility (e.g. multiparty computation and federated analytics), and there are places where these technologies are being deployed in health research contexts today.[23]

[22] Gross and Miller, 2020.
[23] Rieke et al., 2020.

Alternatives and Future Directions

Keeping Data Decentralized

For example, wearables that are being used for biometric surveillance should store data and perform analytics on an individual's smartphone instead of sending it to the cloud. Where new algorithms or analytics are required, federated learning or related technologies should be explored as ways of preserving privacy. How to best communicate to general users the nature of different technology design choices is an important further area to explore.

Keeping Data Decentralized

Zero-knowledge proofs[24] offer another way to preserve individual privacy. They use advanced mathematics to allow one party to prove the validity of claims based on their data to another party without disclosing the data relevant to the underlying content of their statement. In short, zero-knowledge proofs allow us to perform analysis on data and prove the validity of that analysis to a third-party without revealing to that third party the underlying content.

For example, you could produce a zero-knowledge proof to another party indicating that you are unlikely to be contagious (i.e., you have never been infected, do not have any potentially infected contacts, do not have latent symptoms, or have either an antibody test or vaccine conferring immunity). Notably the party that is verifying this proof can only tell that the proof is valid, but isn't able to discern which of the above conditions you have met. This novel approach has tremendous potential to revolutionize privacy standards for health data in clinical, research, and public health contexts.

A further privacy preserving technology that could be incorporated in wearable device data processing is the **trusted execution environment**.[25] This is a piece of hardware that even the possessor of the

[24] Green, 2014.
[25] Felton, 2019.

hardware cannot peer into, such that an individual can send their data to an external parties' trusted execution environment and have it processed without that third party having access to it. Additionally, trusted execution environments are used to store sensitive information, like biometric or credit card information, in a secure environment locally on our smartphones.

These "black boxes" could allow you to safely send your data off-device, but instead of turning it over to a third party to hold indefinitely and use at their discretion, they allow for specific processing of aggregated data in an inaccessible environment. Once the data is processed, results can be returned to individuals and the data that has been sent to the "black box" is never made available for subsequent use.

For example, a trusted execution environment could be used to aggregate GPS or Bluetooth data from many individuals to determine whether they were following social distancing guidelines. The inputs would be an individual's data, and the output, sent only to them, would be whether they are following the appropriate guidelines or have been in contact with COVID-19 positive individuals. Critically doing so with a trusted execution environment would mean this data would be inaccessible and the identity of all parties involved would be kept private.

Mediating Institutions for Data (MIDs)

Finally, another strategy that is potentially complementary to the technological advances outlined above is the insertion of a mid-level entity that represents users, supervises the use of their wearable data by third parties, and has the power to challenge or revise uses it finds to be in conflict with individual or collective interests and preferences. This is part of a broader strategy that asserts that the ethical use of wearables, insofar as they amass power via surveillance, demands corresponding checks and balances to mitigate the threat of asymmetric power relations. Individuals may not have recourse alone,

Alternatives and Future Directions

Mediating Institutions for Data (MIDs)

but an institution that represented groups of individuals could provide a much-needed check to the otherwise unchecked power of data-collecting entities.

One model that has been proposed for representing individuals' data-related interests is the data union. This heuristic may be aptly applied to support communities using wearables. Data unions' "representatives" may be selected or appointed on a volunteer basis and could provide critical reflection and feedback on how the devices are performing and surface concerns from users' perspectives. The fact that many wearables are truly novel that which may be employed in the COVID-19 response despite clearly being not originally designed for this purpose highlights the importance of ongoing assessment of effectiveness and course-correction of unintended consequences when needed.

The data union's collective bargaining power represents the interests of individuals on a scale that remediates some of the currently unsurmountable asymmetries of power over data between users and third-party governments, corporations, etc. The data union could be built into the governance structure of the wearable data management systems and offer a living check-and-balance mechanism to optimize the ethical use of wearable devices and associated data. Further efforts to develop the application of this construct to the wearable space is needed.

The basic setup for data unions applied to wearables would follow the principles laid out by Weyl et. al. regarding Mediating Institutions of Data.[26] We envision an organization (or set of organizations) which collect membership fees from groups of wearable users (e.g., those with Oura rings, Fitbits, etc.) to support full-time employment of user data watchdogs who have relevant expertise and a fiduciary duty to serve the members they represent, and whose job it would be to continuously supervise the third-party uses of user data. This supervision would not only detect and challenge uses which are not

[26] Lanier and Weyl, 2018.

Alternatives and Future Directions

Mediating Institutions for Data (MIDs)

acceptable to the users, but would also be suited to recognizing potential sources of value from user data and negotiating on users' behalf regarding the terms of service which are acceptable and favorable to both third parties (corporations, governments, etc.) and users themselves. In circumstances where third parties' use of data may be systematically harmful to users, the union leadership would be responsible for notifying users and taking measures such as legal action and/or terminating use of users' data. To realize this solution of applying labor law to the production of wearable data, additional and likely new legal instruments would need to be developed specifically designed to protect data from wearables.

Ideally, the data unions could negotiate terms of service on users' behalf and then receive third-party requests to access data, and monitor ongoing use by permissioned parties. However, when unions may be added to existing data exchange relationships, they would be charged with assessing existing terms of service and third-party data uses, with the goal of bringing previously established data relationships in line with equitable, just, and mutually beneficial treatment of user data. A critical corollary to the advancement of wearable user data unions would be codification of these principles and protection in civil law.

05 Conclusion

Wearable devices may be here to stay, however, for their use to be ethical and promoting individual and collective rights and interests they must be approached with the above considerations in mind. Furthermore, our legal and social institutions were not made with these technologies in mind. Currently there exists a legal gap in the protections afforded to data from wearables that must be closed to allow the potential for optimizing the health of individuals and communities while protecting against the risk of undermining basic freedoms and human dignity. The technological and organizational solutions we have proposed meet the ethical requirements of respect for individual autonomy and data privacy and also exemplify a paradigm shift towards the ethical design and use of wearables. A key challenge in this regard is to convey the ethical significance of these sophisticated technologies to consumers who will need to trust the data ethics and governance behind devices that may otherwise look identical to existing models.

Wearables may complement or supplement widespread COVID-19 testing and immunity certificate models in the effort to promote safe reopening and ongoing pandemic response during subsequent waves. The fact that they are already disseminated among many populations, rather than being contingent upon new supply chain production (e.g., for antibody tests, vaccines, etc.), gives them a strategic advantage and makes them likely targets to be implemented in the pandemic response. However, we have also highlighted the potential dangers of redeploying existing wearable technology without appropriate ethical, legal, or social safeguards for individuals' rights and interests regarding their data. Indeed, the solutions we propose have implications beyond the COVID-19 setting and could strengthen the privacy protections in all domains where personal data is collected through digital means.

Expedient implementation of the strategies outlined above is contingent upon the ability to retrofit current wearable devices to employ these novel technological and organizational structures. Moreover,

Conclusion

the privacy preserving technologies outlined above are at different stages of maturity; zero-knowledge proofs and trusted execution environments in particular will need further development before they are ready for use at scale. Nonetheless we believe it is important to acknowledge the unique nature of wearables as data collection tools and to be mindful of the ethical challenges to which they give rise. We call for further attention to the unique role wearables may have in fighting COVID-19 as an opportunity to ensure that wearables are ethically employed, with potential to create standards that will apply broadly to the multitude of current and future wearable uses.

Acknowledgment: The authors wish to express their gratitude to Vince Kuraitis, JD, MBA, Joel Schwarz, JD, CIPP, Joshua Rubin, JD, MBA, MPP, MPH, and Alison Stanger, PhD, for their helpful comments on the early drafts of this paper.

06 References

BBC. 2020. “Coronavirus: People-Tracking Wristbands Tested to Enforce Lockdown.” *BBC News*, April 24, 2020. https://www.bbc.com/news/technology-52409893 (accessed May 10, 2020).

Cozzens, Tracy. 2020. “19 Countries Track Mobile Location to Fight COVID-19.” *GPS World*, March 26, 2020. https://www.gpsworld.com/19-countries-track-mobile-locations-to-fight-covid-19/ (accessed March 28, 2020).

Cranor, L., and M. McDonald. 2008. “The Cost of Reading Privacy Policies.” *I/S: A Journal of Law and Policy for the Information Society* 4, no. 3 (Winter): 543–568.

Felton, Don. 2019. “What Is a Trusted Execution Environment (TEE)?” *Trustonic*, July 5, 2019. https://www.trustonic.com/news/technology/what-is-a-trusted-execution-environment-tee/ (accessed May 17, 2020).

Green, Matthew. 2014. “Zero Knowledge Proofs: An Illustrated Primer.” *Cryptography Engineering*, November 27, 2014. https://blog.cryptographyengineering.com/2014/11/27/zero-knowledge-proofs-illustrated-primer/ (accessed May 17, 2020).

Gross, Marielle S., and Robert C. Miller Jr. 2020. “Federated Learning: Collaboration Without Compromise for Health Care Research.” *Stat*, February 13, 2020. https://www.statnews.com/2020/02/13/federated-learning-safer-collaboration-health-research/ (accessed May 16, 2020).

Hamilton, Isobel Asher. 2020. “Compulsory Selfies and Contact-Tracing: Authorities Everywhere Are Using Smartphones to Track the Coronavirus, and It’s Part of a Massive Increase in Global Surveillance.” *Business Insider*, April 14, 2020. https://www.businessinsider.com/countries-tracking-citizens-phones-coronavirus-2020-3 (accessed on May 15, 2020).

Hong Kong Government. 2020. “‘StayHomeSafe’ Mobile App User Guide.” Leaflet, no date. https://www.coronavirus.gov.hk/eng/stay-home-safe.html

Khan, Mohammed Mujtaba. 2020. “Liechtenstein Rolls out Radical COVID-19 Bracelet Programme.” *Financial Times*, April 15, 2020. https://www.ft.com/content/06b7e6f3-a725-4eda-9153-e0af48040e30

Lanier, Jaron, and E. Glen Weyl. 2018. “A Blueprint for a Better Digital Society.” *Harvard Business Review*, September 26, 2018. https://hbr.org/2018/09/a-blueprint-for-a-better-digital-society

Miller, Robert C., Jr., and Marielle S. Gross. 2019. “Thinking ‘Oat’ of the Box: Technology to Resolve the ‘Goldilocks Data Dilemma.’” *The Health Care Blog*, posted September 9, 2019. https://thehealthcareblog.com/blog/2019/09/09/thinking-oat-of-the-box-technology-to-resolve-the-goldilocks-data-dilemma/ (accessed May 15, 2020).

References

OECD. 2020. "OECD Policy Responses to Coronavirus (Covid-19). Tracking and Tracing COVID: Protecting Privacy and Data while Using Apps and Biometrics." Last updated April 23, 2020. http://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics-8f394636/ (accessed May 3, 2020).

OURA. 2020. "USCF TempPredict Study." https://ouraring.com/ucsf-tempredict-study (accessed May 14, 2020).

Parker, Michael. J., Christophe Fraser, Lucie Abeler-Dörner, and David Bonsall. 2020. "Ethics of Instantaneous Contact Tracing Using Mobile Phone Apps in the Control of the COVID-19 Pandemic." *Journal of Medical Ethics*, published online first, May 4, 2020. doi: 10.1136/medethics-2020-106314 (accessed May 5, 2020).

Pascalev, Assya. 2018. "2567 OHRP meets ToS: Cloud-based technologies in human subject research." *Journal of Clinical and Translational Science* 2, no. S1 (June): 85. doi:10.1017/cts.2018.294

Rieke, Nicola, et al. 2020. "The Future of Digital Health with Federated Learning."*arXiv* preprint , March 18, 2020. DOI: arXiv:2003.08119

Sanger, David E. "Grindr Is Owned by a Chinese Firm, and the U.S. Is Trying to Force It to Sell." *New York Times*, March 28, 2020. https://www.nytimes.com/2019/03/28/us/politics/grindr-china-national-security.html

Satter, Raphael. 2020. "To Keep COVID-19 Patients Home, Some U.S. States Weigh House Arrest Tech." *Reuters, Technology News*, May 7, 2020. https://www.reuters.com/article/us-health-coronavirus-quarantine-tech/to-keep-covid-19-patients-home-some-us-states-weigh-house-arrest-tech-idUSKBN22J1U8 (accessed May 7, 2020).

Smith, Adam. 2020. "Using Big Tech to Tackle Coronavirus Risks Swapping One Lockdown for Another." *The Guardian*, April 22, 2020. https://www.theguardian.com/commentisfree/2020/apr/22/using-big-tech-to-tackle-coronavirus-risks-swapping-one-lockdown-for-another (accessed April 23, 2020).

Solove, Daniel J. 2013. "Introduction: Privacy Self-Management and the Consent Dilemma." *Harvard Law Review* 126, no. 7 (May): 1880–1903.

Valentino-DeVries, Jennifer, Natasha Singer, and Aaron Krolik. 2020. "Scramble for Virus Apps That Do No Harm." *New York Times*, April 29, 2020. https://www.nytimes.com/2020/04/29/business/coronavirus-cellphone-apps-contact-tracing.html (accessed April, 29, 2020).

References

Woodhams, Samuel. 2020. “COVID-19 Digital Rights Tracker.” *Top10VPN*, March 20, 2020; updated May 12, 2020. https://www.top10vpn.com/research/investigations/covid-19-digital-rights-tracker/ (accessed May 12,2020).

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs Books, 2019.