A Practical Privacy Paradigm for Wearables

By Christopher Wolf, Jules Polonetsky, and Kelsey Finch
Future of Privacy Forum*
January 8, 2015

Introduction

Throughout the United States and around the world, consumers are beginning to rely on devices and technologies that take advantage of the Internet of Things, the growing network of connected objects uniting the digital and physical worlds. Within the Internet of Things market, one of the fastest growing segments is wearable devices, estimated to grow from 22 million shipments in 2014 to 135 million by 2018.[1] Fitness bands and smartwatches are the most popular wearables today, but smart clothing, glasses, jewelry, clip-ons and wearable cameras, among others, are all poised for rapid consumer adoption in the coming years.[2]

Designed for ubiquitous use wearables are highly personalized devices that hold the potential to greatly improve consumers' lives – but also the potential to raise new privacy and security risks.[3] Responding to consumer desires and demand, wearable devices deploy a wide range of sensors to collect new or increasingly sensitive environmental, behavioral and social data for and from their users. Data output from these devices is already generating substantial benefits for individual users and society generally, such as helping individuals manage their fitness, exercise and biofeedback, improving personal productivity and efficiency, and making other technologies

* The Future of Privacy Forum is a Washington, D.C.-based think tank whose mission is to advance responsible data practices. The forum is led by Internet privacy experts Jules Polonetsky and Christopher Wolf and includes an advisory board of leading figures from industry, academia, law and advocacy groups.

[1] *See Smartwatches and Smart Bands Dominate Fast-Growing Wearables Market*, CCS Insight (Aug. 2014), http://www.ccsinsight.com/press/company-news/1944-smartwatches-and-smart-bands-dominate-fast-growing-wearables-market.

[2] *See* Juniper Research, Smart Wearable Devices: Fitness, Glasses, Watches, Multimedia, Clothing, Jewellery, Healthcare & Enterprise 2014-2019 (Aug. 9, 2014).

[3] *See* Edith Ramirez, Opening Remarks, Privacy and the IoT: Navigating Policy Issues, International Consumer Electronics Show (Jan. 6, 2014), *available at*http://www.ftc.gov/system/files/documents/public_statements/617191/150106cesspeech.pdf; Julie Brill, Opening Remarks, Federal Trade Commission Spring Privacy Series: Consumer Generated and Controlled Health Data (May 7, 2014), *available at* http://www.ftc.gov/system/files/documents/public_events/195411/2014_05_07_consumer-generated-controlled-health-data-final-transcript.pdf.

simpler and easier to use.[4] In general, proponents of measuring ordinary life and the "Quantified Self" believe that technological self-tracking, such as through wearable devices, will enable new fronts for self-knowledge and self-advancement.[5] That same data, if not properly protected, or if used in unethical or illegal ways, could be used to put individuals' privacy at risk. Critics worry that consumers could find themselves discriminated against by employers or insurers on the basis of their self-generated information, or have their reputations damaged or their safety put at risk by a data breach.

At this early stage in their development, it is difficult to fully predict what the opportunities or risks of wearable devices will be. In many cases, traditional Fair Information Privacy Practices (FIPPs) will aptly address wearables' privacy and security issues, because there will be opportunities for familiar consumer notice and choice mechanisms and other key privacy elements. In other cases, however, there will need to be more common sense applications of these elements.

As the FTC Chairwoman Edith Ramirez recently noted, "We are on the cusp of a new technological revolution" with "an important opportunity to ensure that new technologies with the potential to provide enormous benefits develop in a way that also protects consumer information."[6] We agree that important steps can be taken now to address privacy and security issues in the evolving world of wearables. However, rigid or premature reactions to wearable devices risks both over- and under-protecting individuals' privacy at great cost to innovation and society. We must recognize the complexity of this innovative industry and adapt our protections accordingly to encourage the evolution of equally innovative data protection methods.[7] This paper examines the need for forward-thinking, flexible applications of traditional privacy principles and protections to safeguard individual privacy while wearable technologies and norms continue to mature.

The Future of Wearables

While the widespread adoption of consumer wearable devices promises improvements in health, safety, productivity and entertainment for both individuals and society at large, there remains much we do not yet understand about how they will fit into our economy our lives.

---

[4] *See Wearable Technology Future is Ripe for Growth among Millenials, Says PwC US*, PRNewswire (Oct. 21, 2014), http://www.prnewswire.com/news-releases/wearable-technology-future-is-ripe-for-growth--most-notably-among-millennials-says-pwc-us-515861911.html.

[5] *See* Gary Wolf, *Know Thyself: Tracking Every Facet of Life, from Sleep to Mood to Pain, 24/7/365*, Wired (June 22, 2009), http://archive.wired.com/medtech/health/magazine/17-07/lbnp_knowthyself?currentPage=all.

[6] Ramirez, *supra* note 3.

[7] To illustrate the complexity of negotiating consumer protection and product design in the Internet of Things, consider MIT Professor David Rose's proposal for an Internet of "Enchanted Objects." Rather than extending the current IOT, which Rose critiques as cold, passive, impolite, and isolating, he proposes designers turn ordinary objects into extraordinary ones that "evoke[] an emotional response from you and enhance[] your life." While such designs may have wide appeal, we must also appreciate a critique from Evan Selinger, warning that overly-enchanted devices may undermine both consumers' privacy and their agency. As the IOT matures, we must continue grappling with the full range of social, technological, and legal issues that arise. *See* Evan Selinger, *Too Much Magic, Too Little Social Friction: Why Objects Shouldn't be Enchanted*, Law Rev. of Books (Jan. 8, 2015), http://lareviewofbooks.org/review/much-magic-little-social-friction-objects-shouldnt-enchanted/.

The rapid pace of technological innovation today makes it difficult to predict what wearables will look like in even a few years, let alone to govern how they should collect, use and store information. In just a few years the wearables market has shifted from clip-on devices with basic accelerometers to flexible wristbands, chest straps and smartwatches with accelerometers, altimeters, gyroscopes, ambient light sensors and heartbeat sensors.[8] Future technological advancements may bring devices and sensors even closer to consumers: in clothing, prosthetics, dermal patches, contact lenses, tattoos, implants, and even "swallowable" gadgets.[9] A clip-on pedometer that can be easily removed or deactivated obviously carries different privacy and security risks than a futuristic biometric sensor embedded literally under the skin. Premature regulation at an early stage in wearable technological development may freeze or warp the technology before it achieves its potential, and may not be able to account for technologies still to come.

As wearable technologies gather more and novel types of information, new privacy and design sensitivities will also continue to arise. While many wearable devices collect information about users' health and fitness, for example, more than one type of quantified-self data exists, each with its own level of sensitivity and potential privacy or security impacts. A mobile app that measures only the number of steps a consumer takes in a day requires less privacy engineering than a wearable device that measures blood sugar levels. Any approach to managing privacy risk for such devices must be flexible enough to take these varied sensitivities into account.

Further, as new types of data are more widely collected, new sensitivities around their uses likely will continue to arise. Consumers are choosing to collect, analyze and share data about themselves in new ways and for new purposes every day. Consumers are already utilizing fitness data from wearables for their medical rehabilitation programs, insurance discounts, and employee benefits, as well as for personal use, each of which may raise different privacy and civil liberties concerns.[10] Given that some uses are inherently more sensitive than others, and that there may be many new uses still to come, flexibility will be critical going forward.

While wearable devices and sensors continue to get cheaper and smaller, the number of uses we have for them continues to grow. Wearables already serve a wide variety of primary uses, including individual fitness and health tracking, environmental monitoring, photography, life coaching, navigation, communication and entertainment, art, and assistive services.[11] They also support a wide range of secondary purposes, including invaluable medical and social sciences research. And app developers also begin to advance into the wearable space, they bring even more innovation and personalization to these devices. The sheer variety of useful data produced by wearable devices – and the even more diverse array of interfaces through which consumers interact with them – requires a common sense approach that ensures consumer protection as well as ensures that these tools and the data they provide will be practically available.

---

[8] *See* Juniper Research, *supra* note 2; Jody Ranck, The *Wearable* Computing Market: A Global Analysis 6 (July 2012), *available at* http://go.gigaom.com/rs/gigaom/images/wearable-computing-the-next-big-thing-in-tech.pdf.
[9] *Id.*
[10] *See* Paolo Bonato, *Advances in Wearable Technology and Applications in Physical Medicine and Rehabilitation*, 2:2 J. NeuroEngineering & Rehabilitation (2005); Parmy Olson, *Wearable Tech Is Plugging into Health Insurance*, Forbes (June 19, 2014), http://www.forbes.com/sites/parmyolson/2014/06/19/wearable-tech-health-insurance/.
[11] *See Wearable Technology Application Chart*, Beecham Research http://www.beechamresearch.com/article.aspx?id=20 (last visited Dec. 15, 2014).

Wearing the FIPPs

Traditional privacy practices and principles, such as the Fair Information Practice Principles (FIPPs), continue to provide the core guidelines for the Internet of Things, including wearable devices. The FIPPs do not establish specific rules prescribing how organizations should provide privacy protections in all contexts, but rather provide high-level guidelines. [12] Over time, as technologies and the global privacy context have changed, the FIPPs have been presented in different ways with different emphases.[13] Accordingly, we urge policymakers to enable the adaptation of these fundamental principles in ways that reflect technological and market developments.

At their core, the FIPPs articulate basic protections for handling personal data. Important principles include: (1) notice, (2) choice, (3) purpose specification, (4) use limitation, and (5) data minimization.[14] By their very nature, wearable technologies require frequent, often continuous, data inputs and transmissions from other connected devices and external data sources. A rigid application of the FIPPs could inhibit these technologies from even functioning, and while privacy protections remain essential, a degree of flexibility will be key to ensuring the Internet of Things can develop in ways that best help consumer needs and desires.

The need for a common sense approach may be most apparent with regards to the principles of notice and choice. These principles remain at the foundation of current privacy protection frameworks, but may in many cases need to be implemented in new ways. As the Commission has recognized, "companies should give consumers clear notice and provide simplified choices for unexpected collection or uses of their data," but "providing notice and choice in an IoT world is easier said than done."[15] Wearable devices and other Internet of Things applications frequently feature small screens or user interfaces, or no screens at all.[16] Similarly, some devices are capable of just-in-time notices, while for others such a concept may be impossible to implement. Moreover, some of these interactions are routine and anticipated by users; some of the information being shared and collected by these devices and technologies may not be personally identifiable or present few privacy issues for consumers. Other uses may be determined to be beneficial to the user or society and create such a low risk of harm that notice might be handled

---

[12] *See, e.g.*, The White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (2012); FTC, Protecting Consumer Privacy in an Era of Rapid Change (2012).

[13] *See id.*; Edith Ramirez, The Privacy Challenges of Big Data: A View from the Lifeguard's Chair, Keynote Address by FTC Chairwoman Edith Ramirez, Technology Policy Institute Aspen Forum (Aug. 19, 2013), *available at* http://www.ftc.gov/speeches/ramirez/130819bigdataaspen.pdf.

[14] *See, e.g.*, OECD, OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data 14 (2013), *available at* http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf; The White House, *supra* note 9, at 10.

[15] Ramirez, *supra* note 3.

[16] *See* Will Knight, *What Comes After the Touch Screen?*, MIT Tech. Rev. (Oct. 11, 2012), http://www.technologyreview.com/news/429546/what-comes-after-the-touch-screen/.

in a flexible manner. Wearable devices require challenging decisions to be made about how to best provide consumers with notice and other relevant information about data use.[17]

Thus, while many wearables will continue to provide notice through traditional registration pages, mobile app or desktop interfaces, other forward-thinking alternatives should also be considered and supported. Wearables offer consumers the opportunity to interacting with their devices not just through sight and sound, but through touch and touch feedback: soon, they will be able to "give us tactile feedback exactly where we touch it (instead of vibrating the entire device), will differentiate the left from the right in a navigation application, will pulse on the arm wrist as a real pulse during an emotional exchange, will give us alerts identifying tactily who is calling, will give us the tactile hit when we play a game, and many more cool yet natural experiences."[18] As these haptic technologies begin to flourish, allowing wearables to "buzz, vibrate, or otherwise 'communicate information through people's skin,'" new ways to communicate about privacy can also emerge.[19] Wearable technologies, for example, can provide notice of data collection through visual, auditory or tactile clues such as lights or vibration that may indicate when a device is active or data is being collected.

In some situations, however, more prominent or interruptive notices may not be feasible or provide little benefit to consumers, depending on the nature of the nature of the privacy risk and the utility value arising from a particular function. It could be reasonable, for example, to design a smart sneaker with an embedded pedometer to collect step information by default, without necessarily needing additional just-in-time notifications. Whether data collection is low-risk or is expected by consumers are simply factors that should continue to influence what kinds of privacy notices consumers receive.

Consent requirements must also be practically applied to the Internet of Things. The Internet of Things is a construct built upon the connections among a multitude of different connected devices and sensors. These connections allow for information to be shared in both public and private spaces. Requiring individuals to manually give consent to each of these potential interactions may be impractical for some devices. Further, because wearable devices are, by definition, visibly and voluntarily worn by users, a wider range of contextual privacy choices is available to their users, including simply removing the device as desired.

Purpose specification and use limitation requirements are intertwined and typically require organizations to specify how data is to be used at or before the time of collection and then to use data only for those specific purposes. While important principles to protect consumer expectations, they may also foreclose the ability to maximize applications of the Internet of Things that are not immediately foreseen. Beyond the primary purpose for collecting data there could exist any number of positive, unexpected applications. For example, consumer-generated wellness information is of significant interest to the research community, and the integration of

---

[17] *See* Research Group of the Office of the Commissioner of Canada, Wearable Computing – Challenges and Opportunities for Privacy Protection (Jan. 2014), https://www.priv.gc.ca/information/research-recherche/2014/wc_201401_e.pdf.

[18] *Id.*

[19] *See* Clive Thompson, *Soon Your Tech Will Talk to You Through Your Skin*, Wired (Dec. 22, 2014), http://www.wired.com/2014/12/haptic-technology/.

this data into an individual's electronic health records could offer much improved health outcomes and treatments.[20]

When appropriate, companies should endeavor to minimize the amount of identifiable information that is collected, stored, and used. However, strict data minimization may not be practical or ideal with regards to all Internet of Things and wearable technologies. As discussed, data fuels much of the functionality of wearable devices, and traditional methods of data minimization that impose strict restrictions on the collection of personal information may not be feasible. In fact, a key value of the Quantified Self movement is the collection of a "360-degree view" to gain insights from the interaction of any self-generated data that might affect the individual.[21] Furthermore, some of the data generated by the Internet of Things may blur the line between personal and non-personal information. As a result, robust technical and administrative de-identification procedures should be used in place of rigid data minimization requirements.

Finally, we agree with Chairwoman Ramirez's recent remarks questioning "the notion that we must put sensitive consumer data at risk on the off-chance a company might someday discover a valuable use for the information." But we also believe that novel data uses do sometimes develop from data collection that is based on speculative or "pure research" purposes and that allowing for these uses is essential. By its very nature, big data anticipates extracting unexpected insights from the types of datasets that might be created by consumers utilizing their wearables to ubiquitously track their own activities. The societal benefits of allowing for secondary research of this type have been recognized in many circumstances. For example, just this fall the National Science Foundation sponsored a five-year project by Carnegie Mellon University to "improve educational outcomes and advance the science of learning . . . by accessing more than 550 datasets generated from interactive tutoring systems, educational games and massively open online courses."[22] Consumer-generated data from wearables, appropriately secured and utilized, could prove equally valuable to public and private research in education and other fields, as well as health and wellness projects already underway.[23]

Rigid application of data minimization rules might ignore those circumstances where the rewards of collecting and handling data in a certain manner outweigh its risks.[24] As we explain later, we believe that significant data decisions, such as those regarding new uses or data minimization, can be assessed and balanced through serious and systematic risk-benefit assessments, using

---

[20] In addition to new healthcare technologies and treatments derived from or based on consumer-generated data, the proliferation of consumer-generated data has sparked a new wave of consumer engagement with their own self- and professional care. National eHealth Collaborative, Patient-Generated Health Information, Technical Expert Panel Final Report (Dec. 2013), http://www.healthit.gov/sites/default/files/pghi_tep_finalreport121713.pdf.
Even within the traditional medical context, consumer-generated data "provides an opportunity to capture needed information for use during care, with potential cost savings and improvements in quality, care coordination and patient engagement." *Id.*

[21] *See Counting Every Moment*, The Economist, Mar. 3, 2012, *available at* http://www.economist.com/node/21548493.

[22] Press Release, *Carnegie Mellon Leads New NSF Project Mining Educational Data to Improve Learning*, Carnegie Mellon U. (Oct. 2, 2014), https://www.cmu.edu/news/stories/archives/2014/october/october2_learnsphere.html.

[23] *See* Sorenson Research, Smart Wearable Healthcare Report 2014, http://www.soreonresearch.com/wearable-healthcare-report-2014/.

[24] See below for further discussion of how organizations can engage in such Benefit-Risk Analysis with consumer data.

quantitative methodologies such as privacy impact assessments and data benefit analyses. Furthermore, this process of identifying and balancing both benefits and risks fits squarely within the FTC's current consumer protection activities under its Section 5 unfairness authority.

A Flexible, Use-Focused Wearables Paradigm

As we have argued previously, there are times when collection limitations are appropriate, but at other times the more effective way to ensure that benefits are achieved and privacy risks are minimized will be with a paradigm that focuses on data uses.[25] This paradigm relies on the following proposals.

Respect for context. According to the White House Consumer Privacy Bill of Rights, the respect for context principle means that "consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data."[26] This principle is often interpreted to mean that personally identifiable information should be used only in ways that individuals would expect given the context of the collection, such as to fulfill orders or engage in first-party marketing. However, focusing exclusively on individual expectations would curtail unexpected new uses or research breakthroughs that may arise from consumer-generated data. For example, analyzing behavioral patterns or biometrics data from a fitness tracker, originally collected in order to report basic wellness information to the user, may yield unanticipated health insights that could be provided individually to users or used in the aggregate to advance medical knowledge. Not all secondary uses will yield such benefits, however, and in circumstances where these benefits are too remote or infringe too much on consumers' privacy, such uses would not be appropriate. Still, rigidly and narrowly specifying context could trap knowledge that is available and critical to progress.

At this early stage in wearables' development, however, what "context" means for consumers and what they reasonably expect from their wearable devices remains open questions. Firstly, wearable devices may collect data in a variety of ways: consumers may voluntarily input information into the device, such as what they are eating or how much they weigh; the device's sensors may read and record external stimuli, such as air quality or ambient light; or the device's software may even automatically incorporate data from other apps, devices, sensors, or information feeds, such as social media. Each input carries its own considerations, including consumer expectations about data accuracy and utility.

Furthermore, how wearable devices interact with their users, with each other, and with their environments has yet to be determined. Wearables are bringing data collection and usage into new physical and social spaces, and what consumers expect from their devices in these contexts

[25] Christopher Wolf & Jules Polonetsky, An Updated Privacy Paradigm for the Internet of Things (Nov. 19, 2013), *available at* http://www.futureofprivacy.org/wp-content/uploads/Wolf-and-Polonetsky-An-Updated-Privacy-Paradigm-for-the-%E2%80%9CInternet-of-Things%E2%80%9D-11-19-2013.pdf.

[26] Executive Office of the President, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (Feb. 2014), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

is still changing day by day.[27] When wearables (such as smart textiles) are still novel to consumers and their interactions with other devices are still being imagined or negotiated, their "context" – and consumers' expectations for that context – will be malleable. For example, we may learn that consumers expect their wearables to automatically share data with their smart-home devices, so that their thermostat can adjust the temperature as they move from room to room or so that their doors can lock when they leave the house. Or, consumers with a particular fitness wearable might expect it to communicate with a smart-sneaker from the same brand. Other interactions, such as between that smart-sneaker and another company's smart-home thermostat, consumers may *not* expect, though this too could change over time.[28] Wearables remain at an early stage in both technological development and consumer adoption: how consumers expect and want their devices to act in a range of circumstances continues to change. While "context" norms continue to be explored, wearables should be guided by traditional notions of fairness and consumer protection principles.

Other context variables should be also considered, such as whether the expected uses of data are beneficial for the consumer or society at large or whether they might have negative impacts. Developing a richer understanding of potential impacts of uses of data should be a priority for companies, policymakers, and third party organizations, and curtailing harmful uses should be the underpinning of any regulatory efforts and product developments alike.

Benefit-risk analysis. In the era of Big Data, wearables' capacity for granular, ubiquitous data collection opens the door to new and important health, efficiency, and personal benefits – but, at the same time, to equally significant privacy risks. As discussed above, a rigid application of data minimization principles to wearables would stymie unexpected but valuable breakthroughs in health research, sustainable development, energy conservation, and personalized marketing. At the same time, this does not mean that any and all sensitive personal data should be held perpetually on the off-chance it may someday become valuable. Instead, organizations must conduct serious assessments of the possible benefits of using data and weigh those benefits against the possible risk to consumer privacy.[29]

Responsible organizations regularly engage in systematic Privacy Impact Assessments (PIAs) to identify and address privacy issues. However, calculating the privacy risk is only one part of the equation: decision-makers also need to engage in a Data Benefit Analysis (DBA), in order to account for the sizeable variance in anticipated big data benefits. We have previously proposed "a methodology to better structure the discussion of big data benefits, assessing such variables as the *nature* of the benefit, the *identity* of the beneficiary and the *likelihood* of success. The results of this process, in turn, will feed into existing PIA practices to form a balanced, comprehensive view of big data risks and rewards."[30] While not every issue or data practice will require a DBA, by engaging in this sort of systematic review, organizations will be better able to address the

[27] At the 2015 International Consumer Electronics Show, companies debuted wearables "designed for everything from baby monitoring to calmer meditation." Rachel Metz, *CES 2015: Wearables Everywhere*, MIT Technology Review (Jan. 5, 2015), http://www.technologyreview.com/news/533916/ces-2015-wearables-everywhere/.
[28] *See* Jules Polonetsky & Omer Tene, *A Theory of Creepy: Technology, Privacy and Shifting Social Norms*, 16 Yale L.J. & Tech. 59, 91 (2013), http://pacscenter.stanford.edu/sites/all/files/Theory_of_Creepy_1.pdf.
[29] *See* Jules Polonetsky, Omer Tene & Joseph Jerome, *Benefit-Risk Analysis for Big Data Projects* (Sept. 2014), http://www.futureofprivacy.org/wp-content/uploads/FPF_DataBenefitAnalysis_FINAL.pdf.
[30] *Id.*

novel data and novel data uses arising from wearables, even in the face of their rapid technological advancement.

Transparency. In order to bolster practices that respect the context of data collection, organizations also must be transparent about the ways in which they use consumers' personal information. Organizations may not be able to predict all of the ways in which consumer information may be used, but they can provide details about the primary and secondary uses that are planned, such as to improve the wearable product, to maintain device security, to provide analytics or serve advertisements, or to conduct or contribute to research. If certain data are not used for particular purposes, that could also be important to disclose to consumers.

Moreover, there exist special sensitivities for certain uses of consumer data, such as devices owned by, and sharing data with, employers, insurers or others making eligibility decisions. While organizations should disclose when and how such information is used to make decisions that impact individuals or shape their experiences, further exploration is warranted before the imposition of broad prescriptive rules against particular uses of wearable data. As companies' and consumers' expectations with regard to these uses are still developing, transparency practices become all the more important.

De-identifying data. One of the strongest mechanisms to protect personal information is to render it non-personal, or de-identified. By decoupling an individual's identity from their data through technical means, often buttressed by administrative protection, de-identification minimizes or eliminates most privacy risks. Importantly, de-identification allows for organizations to use and maintain – and in some cases share or publish – valuable data sets, even those based on sensitive personal information, such as health data or geolocation records. This in turn enables critical public and private research, product support and maintenance, and the development of new services. We strongly support de-identification standards that recognize both reasonable technical and administrative controls, as well as enhanced transparency for consumers to better understand how the de-identification of their data has been achieved.[31]

However, given the complexities of the wearable ecosystem and the evolution of new de-identification and re-identification techniques, whether a specific de-identification practice is appropriate will depend on the circumstances. Whether there are certain contexts in which consumer-generated data could or should be de-identified or technically obscured as a matter of policy requires further investigation and discussion.

Reasonable individual access. Although not all wearable devices will lend themselves towards easy user access to the information they collect, allowing users to engage with their own data will encourage trust in the wearables ecosystem. While some consumers may prefer to keep their information private, others may prefer to share their data with a family member or caretaker. Enabling such choices empowers consumers to engage more deeply in their own self-care. We have long supported efforts by organizations to offer tools that allow users to add, tailor, or featurize their data, such as by providing them access to portable, machine-readable copies of

[31] *See* Yianni Lagos & Jules Polonetsky, *Public vs. Nonpublic Data: The Benefits of Administrative Control*, 66 Stan. L. Rev. Online 103 (2013), http://www.stanfordlawreview.org/online/privacy-and-big-data/public-vs-nonpublic-data.

their data, or by providing access via third-party programming interfaces. However, organizations will need to take into account utility, security and data minimization issues to determine what reasonable access to data is for particular products or services.

Appropriate security. Wearable devices that may contain detailed and long-term records of an individual's behaviors, communications, movements, activity levels, environments and precise health status must be appropriately secured. While different wearables may face distinct threat models, organizations should be prepared to defend consumers' personal data against both internal threats, such as curious employees, and external threats, such as hackers or scammers. Given their high level of connectivity, it is also important that wearable data be adequately protected at rest on the device, in transit, and in the cloud or anywhere else they reside. Device manufacturers or app developers should also consider how they wish to respond to government requests for wearable data, when designing their programs' security and technical specifications. Common security principles and standards that can adapt to rapid technological advancements, as well as means to share information about new threats, should also be developed to support strong, industry-wide data security.

Develop codes of conduct. Finally, underlying the flexible application of fundamental privacy principles should be self-regulatory codes of conduct. Such codes have proven to be the most effective way to protect privacy without stifling innovation in other burgeoning fields, including the now-abundant mobile application ecosystem. Even given the rate technological and commercial innovation in the wearables space, codes of conduct that establish practical and consistent privacy frameworks could enable businesses large and small to protect consumers' privacy and preferences. It is important that codes of conduct or best practices for wearables reflect not only our fundamental privacy principles and laws, including the FIPPs, but also be tailored to the technological and practical realities of the Internet of Things and the evolving social norms and preferences of their users.

In continuation of its pioneering work on codes of conduct and in the wearables space, FPF has convened a Working Group dedicated to wearables and consumer-generated health data. The group will focus its efforts on establishing common understanding and rules around some of the critical issues identified above, including: the scope of consumer-generated data, consent for sharing, pragmatic de-identification, and general privacy principles for wearable and wellness data.

Compliance programs that can demonstrate accountability and document controls around data access and uses can further help ensure accountability. In the future, automated tools may play an increasing role in strengthening compliance and transparency efforts. Although such technologies are only beginning to enter the market, they hold great promise and will play a key role in the future.[32]

[32] *See, e.g.*, David Harris, *Could this Cambridge Start-up Have Helped Uber Avoid Its Current Privacy Scandal?*, Boston Bus. J. (Nov. 24, 2014), http://www.bizjournals.com/boston/blog/startups/2014/11/could-this-cambridge-startup-have-helped-uber.html?page=all (describing TrustLayers technology which helps companies connect privacy policies and laws with the data they collect).

Finally, we note as well the important role played by the wearable device companies and platforms in this space. Leading mobile operating systems have already instituted specific and sophisticated privacy and security-oriented rules to govern applications for their wearables.[33] These baseline principles provide a helpful starting point for other stakeholders and policymakers as wearable technologies continue to evolve.

Conclusion

There is much work still to be done to determine when and how these privacy principles should be applied to specific wearable devices or to protect certain types of consumer-generated data. Consumers, businesses, and policymakers must all have a voice in deciding how wearables can and should fit into our increasingly interconnected lives.

Moving forward in the wearables space, we urge policymakers to adopt a forward-thinking, flexible application of the FIPPs. In this way we can recognize the often heightened sensitivity of consumer-generated personal data and craft appropriate protections for the growing variety of wearable devices, while also allowing for the use and sharing of this data for societally and individually beneficial purposes.

[33] Apple HealthKit and Google Fit, for example, both prohibit applications from gathering data from their respective platforms for certain purposes, such as advertising. *See HealthKit*, Apple Developer, https://developer.apple.com/healthkit/ (last visited Jan. 5, 2015); *Google Fit Platform Overview*, Google Developers, https://developers.google.com/fit/overview (last visited Jan. 5, 2015).