The Internet of Things as a Tool for Inclusion and Equality

Jules Polonetsky [*]
Stacey Gray [†]

TABLE OF CONTENTS

[*] CEO, Future of Privacy Forum.

[†] Policy Counsel, Future of Privacy Forum.

Adapted from comments filed in June 2016 to the National Telecommunications and Information Association (NTIA) by John Verdi & Chanda Marlowe, Future of Privacy Forum.

I. INTRODUCTION

In the next decade, a critical issue for policymakers and regulators will be the advancement and growing ubiquity of cyber-physical systems, or the Internet of Things (IoT). Consumer-facing IoT systems are already delivering benefits to consumers and society.[1] IoT can also be a powerful tool for inclusion and equality, enabling accessibility for many who have traditionally encountered hardship or exclusion because of physical disabilities or other limitations. Through creative forms of notice and flexible application of the Fair Information Practice Principles (FIPPs), policymakers and regulators can find meaningful ways to protect data privacy while promoting beneficial innovation.

II. THE INTERNET OF THINGS AND PRIVACY

As a threshold matter, not all systems in the Internet of Things (IoT) implicate privacy. While many IoT systems are directly consumer facing, many have little or no connection to individuals. For example, an oil company may install sensors to monitor an Alaskan pipeline,[2] a power generation company may use sensors to predict and avoid potential power failures,[3] and an industrial vendor may collect data from jet engines to monitor the environmental impact of aircraft[4]—all examples of machine-to-machine (M2M) connections that do not collect or reveal information about individuals.[5] Policies aimed towards consumer protection must first distinguish between consumer and non-consumer uses of connected devices if they are to avoid unduly affecting beneficial industrial uses of those devices.

Nonetheless, many IoT systems *do* involve data from or about individuals. Information networks created by IoT promise a wide array of consumer benefits, including improvements in healthcare, efficient traffic management, public safety, convenience, environmental protection, and

[1] *See generally* Peter Newman, *THE INTERNET OF THINGS 2017 REPORT: How the IoT is improving lives to transform the world*, BUS. INSIDER (Jan. 12, 2017, 12:12 PM), http://www.businessinsider.com/the-internet-of-things-2017-report-2017-1 [https://perma.cc/7JE8-GKTT].

[2] *See* Microsoft Corp. Blogs, *Fueling the Oil and Gas Industry with IoT*, MICROSOFT (Dec. 4, 2014), https://blogs.microsoft.com/iot/2014/12/04/fueling-the-oil-and-gas-industry-with-iot/ [https://perma.cc/X225-DKZL].

[3] *See* Dan Woods, *What Is GE Predix Really Building?*, FORBES (Sept. 28, 2016, 6:20 AM), https://www.forbes.com/#6b3810e92254 [https://perma.cc/Y8MR-RFFN].

[4] *See* Bhoopathi Rapolu, *Internet of Aircraft Things: An Industry Set to be Transformed*, AVIATION WEEK NETWORK (Jan. 18, 2016), http://aviationweek.com/connected-aerospace/internet-aircraft-things-industry-set-be-transformed [https://perma.cc/8FX4-C3VT].

[5] *See 50 Sensor Applications for a Smarter World. Get Inspired!*, LIBELIUM (May 2, 2012), http://www.libelium.com/50_sensor_applications/ [https://perma.cc/J57R-3Q4B] (last accessed March 2, 2017).

business innovation.[6] These benefits are enabled when industry is able to layer applications on top of connected devices to create a network of smart systems. Maximizing such benefits necessarily requires collecting, retaining, and sharing information in new ways. Information sharing on the scale generated by IoT implicates privacy risks and security concerns that have not been traditionally associated with consumer devices, such as household items and personal vehicles.[7]

In addition to legal and regulatory frameworks, business-developed standards designed to address security and privacy issues are necessary to ensure that IoT achieves its full potential. If there are lax controls or insufficient oversight of the collection of personal information through connected devices, consumers will lose trust in the evolving technologies. In the words of European Commission Vice-President Neelie Kroes, responsible for the EU Digital Agenda, the industry "cannot innovate in a bubble if citizens are not coming along for the journey."[8]

The Internet of Things raises new issues for the Fair Information Practice Principles (FIPPs), which have long provided the foundation of consumer privacy protection in this country and embody core privacy values.[9] The FIPPs articulate basic protections for handling personal data: (1) Transparency, (2) Individual Control, (3) Respect for Context, (4) Security, (5) Access and Accuracy, (6) Focused Collection, and (7) Accountability.[10] Over time, as technologies and the global privacy context have changed, the FIPPs have been presented in different ways with different emphases.[11] On balance, the FIPPs are not meant to establish rigid

[6] *See generally* MCKINSEY GLOB. INST., THE INTERNET OF THINGS: MAPPING THE VALUE BEYOND THE HYPE (June 2015), http://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/The%20Internet%20of%20Things%20The%20value%20of%20digitizing%20the%20physical%20world/Unlocking_the_potential_of_the_Internet_of_Things_Executive_summary.ashx [https://perma.cc/7KZN-FP99].

[7] Janna Anderson & Lee Raine, *The Internet of Things Will Thrive by 2025*, PEW RES. CTR. (May 14, 2014), http://www.pewinternet.org/2014/05/14/internet-of-things/ [https://perma.cc/GR2L-XF9Y].

[8] Neelie Kroes, Vice-President, Eur. Comm'n responsible for the Dig. Agenda, Speech at the High-level Internet of Things Conference 4 (May 16, 2011), http://ec.europa.eu/information_society/newsroom/cf/document.cfm?action=display&doc_id=827 [https://perma.cc/L8S3-N64T].

[9] *See generally* ORG. FOR ECON. CO-OPERATION & DEV., *infra* note 10; *see also* THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD 1 (Feb. 23, 2012), https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf [https://perma.cc/D23T-EEM8] (applying the FIPPs in a Consumer Privacy Bill of Rights).

[10] *See generally id.*; ORG. FOR ECON. CO-OPERATION & DEV., OECD GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA 14 (2013),https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf [https://perma.cc/C5RL-XJQF].

[11] *See* Edith Ramirez, Chairwoman, Fed. Trade Comm'n, Keynote Address at the Technology Policy Institute Aspen Forum: The Privacy Challenges of Big Data: A View from the Lifeguard's Chair (Aug. 19, 2013), https://www.ftc.gov/sites/default/files/documents/public_statements/privacy-challenges-big-data-view-lifeguard's-chair/130819bigdataaspen.pdf [https://perma.cc/RM9R-E3RU].

parameters for the processing of information but rather to serve as high-level guidelines.

While the traditional mechanisms—such as presentations of detailed privacy policies and prompts for consents—have served to promote the FIPPs in many contexts, new mechanisms may be appropriate for some implementations of the Internet of Things. New issues around the FIPPs can be addressed with openness to flexibility and new forms of notice.

III. THE INTERNET OF THINGS AND INCLUSION

When the non-profit Pew Research Center queried more than 1,600 experts on the subject, 83 percent predicted that IoT will "have widespread and beneficial effects on the everyday lives of the public by 2025."[12] Among other advantages, IoT devices can improve public health by keeping patients in closer touch with doctors, reducing highway deaths by automatically braking vehicles to avoid crashes, and boosting food supplies by helping farmers tend their crops.[13] Moreover, IoT systems can improve the day-to-day quality of life for individuals – even those who are not connected to the Internet, who do not know what IoT is, or who may not be able to afford IoT-enabled technology, including disadvantaged groups and rural communities. Specifically:

A. *For people who are visually impaired*

- OrCam: A wearable video camera that attaches to the wearer's eyeglasses and provides artificial vision technology for the visually impaired. It translates written text to audio in real-time (OrCam MyReader) and recognizes stored faces of individuals and other consumer products (OrCam MyEye).[14]
- Dot: The world's first Braille smart watch, which features a series of dull pins that rise and fall at customizable speeds and allows users to read text messages and e-books.[15]
- Cloud-connected shoe insoles: Developed at MIT Media Lab, works with a mobile device to help the user navigate a city without looking at a smartphone for directions.[16]
- Nest: A home automation system, which allows for control of appliances and home thermostat via smartphone.[17]

[12] Anderson & Raine, *supra* note 7.

[13] *Id.* at 7.

[14] OR CAM, http://www.orcam.com/ [https://perma.cc/C8UL-CC3P] (last visited May 20, 2016).

[15] DOT, INC., https://dotincorp.com/ (last visited May 20, 2016).

[16] Emily Gertz, *Toe Tickling Shoes Let you Navigate the City by Touch*, POPULAR SCIENCE, (May 20, 2016) http://www.popsci.com/article/gadgets/toe-tickling-shoes-let-you-navigate-city-touch [https://perma.cc/N74U-MLCU]. The SuperShoes insoles include small motors that tickle the wearer's toes to indicate which direction to walk, a microcontroller, and a low-power Bluetooth transmitter that wireless connects the insoles with the user's smartphone. *Id.*

- iRobot's Roomba[18]: A smart vacuum cleaner equipped with software and sensors that allow it to efficiently navigate rooms.

B. *For people with mobility-related limitations*

- Smart Home assistants, such as the Amazon Echo or Google Home, that are "always ready" or able to be activated by a wake phrase, allow users to control things in the home remotely, such as lights, door locks, or security systems.[19]
- Connected vehicle technologies, such as General Motor's Super Cruise driver-assistance technology (scheduled to be introduced in 2017 model Cadillacs), can provide semi-autonomous operation.[20]
- Indoor Location Mapping: Allows the user to identify the location of various services, including ramps, accessible services, and escalators and elevators in public places.[21]

C. *For people who are hearing impaired*

- Ring[22]: A connected doorbell and home security solution, which alerts users to motion and allows residents to remotely monitor their door.
- Oticon Opn[23]: A connected hearing aid that can be programmed to communicate with a range of other connected devices, such as smoke detectors, baby monitors, or other smart home devices.

D. *For older adults and the elderly*

- Lively[24]: Sensors that alert relatives when an older family member fails to take medicine, eat, or return home from a walk.

[17] *Nest app—Your Home in Your Hand*, NEST, https://nest.com/app [https://perma.cc/JS55-7WZM] (last visited May 20, 2016); GLOB. INITIATIVE FOR INCLUSIVE INFO. & COMMC'N TECHS, *Internet of Things: New promises for Persons with Disabilities* (July 2015), http://www.g3ict.org/press/press_releases/press_release/p/id_89 [https://perma.cc/Z9GZ-E4EN].

[18] *Roomba–Your Partner for a Cleaner Home,* IROBOT, http://www.irobot.com [https://perma.cc/KPR6-SKUP] (last accessed May 20, 2016).

[19] GLOB. INITIATIVE FOR INCLUSIVE INFO. & COMMC'N TECHS, *supra* note 17.

[20] *Id.;* Paul Stenquist, *In Self-Driving Cars, a Potential Lifeline for the Disabled*, N.Y. TIMES (Nov. 7, 2014), http://www.nytimes.com/2014/11/09/automobiles/in-self-driving-cars-a-potential-lifeline-for-the-disabled.html?_r=0 [https://perma.cc/4B5B-NVYG].

[21] Corinne Iozzio, *Indoor Mapping Lets the Blind Navigate Airports,* SMITHSONIAN.COM (Aug. 8, 2014), http://www.smithsonianmag.com/innovation/indoor-mapping-lets-blind-navigate-airports-180952292/ [https://perma.cc/KPC4-RMF7].

[22] *Never Miss a Visitor,* RING, https://ring.com [https://perma.cc/2MEW-DVKY](last visited May 20, 2016).

[23] Victoria Woollaston, "These Hearing Aids Link to Smart TVs, Doorbells and Smoke Alarms So Wearers Never Miss a Beat", WIRED (Jan. 2, 2017), http://www.wired.co.uk/article/oticon-smart-hearing-aid [https://perma.cc/5QZK-QTHJ] (last visted June 19, 2017).

E. *For those with health concerns*

- Continuous Glucose Monitoring (CGM)[25]: A wearable device that displays a constant reading of blood glucose level by inserting a tiny electrode under the skin which then transmits the glucose reading via wireless radio frequency to a display device. Reports may be shared with parents and with care providers.
- Ralph Lauren's Polo Tech Shirt[26]: A shirt with conductive threads and a small snap-on module that relays information like heart rate and breathing data to a Bluetooth-connected mobile device.

F. *For people who are hospitalized*

- General Electric (GE) Healthcare has developed technology to keep hospitals more sanitary and to reduce medical errors. GE's technology can determine whether soap and sanitizer dispensers are used by medical personnel before and after seeing a patient.[27]
- GE Healthcare technology can also track when patients get in and out of bed to help prevent falls, monitor clinical roundups to ensure that clinicians check on patients at least once per hour, and can help prevent and treat painful pressure ulcers.[28]
- AiCure[29]: A company that combines video facial recognition and artificial intelligence, can help confirm that patients have taken their medication.

[24] *Lively 24/7 Emergency Medical Alert System,* LIVELY, http://www.mylively.com/how-it-works [https://perma.cc/AZC8-PECN] (last accessed May 20, 2016).

[25] *See generally, Continuous Glucose Monitoring,* MEDTRONIC, http://www.medtronicdiabetes.com/products/continuous-glucose-monitoring [https://perma.cc/T2T6-H9YJ] (last accessed May 20, 2016); GLOB. INITIATIVE FOR INCLUSIVE INFO. & COMMC'N TECHS, *supra* note 17.

[26] Tim Moynihan, *Your Next Polo Shirt Could Have an Activity Tracker Built Right In*, WIRED (Aug. 27, 2014 6:30 AM), https://www.wired.com/2014/08/ralph-lauren-polo-tech-shirts/ [https://perma.cc/2F24-C3V8].

[27] *See GE Scientists Develop Multi-sensing Handheld Probe to Assess and Prevent Pressure Ulcer Formation During Hospital Stays*, GE GLOBAL RES. (Mar. 19, 2015), http://www.geglobalresearch.com/news/press-releases/ge-scientists-develop-multi-sensing-handheld-probe-to-assess-and-prevent-pressure-ulcer-formation-during-hospital-stays [https://perma.cc/N7MQ-6ABV]; *GE Healthcare and Summerville Medical Center Hail AgileTrac Success*, GE HEALTHCARE (Apr.12, 2013), http://newsroom.gehealthcare.com/ge-healthcare-and-summerville-medical-center-hail-agiletrac-success/ [https://perma.cc/S43E-CVT9].

[28] *Id.*

[29] *See Ai Cure Technologies is Awarded Patent for Interactive Medication Adherence Monitoring System*, AICURE (Dec. 16, 2013), https://aicure.com/ai-cure-technologies-is-awarded-patent-for-interactive-medication-adherence-monitoring-system/ [https://perma.cc/J48T-BXZ5.].

G. For the economically disadvantaged

- Smart meters offer access to detailed consumption data that can assist customers in managing their energy usage, which may save customers money on their energy bills.[30]
- M2M technology: Expands consumers' access to credit by enabling two new payment methods: pay-as-you-go ("PAYG") asset financing, which allows consumers to pay for products over time and prepaid, where consumers pay for services on an as-needed basis.[31]

H. For farmers in rural communities

- Crop sensors can relay information to application machines, which then release the appropriate amount of fertilizers and pesticides.[32] Soil sensors can provide similar information leading to efficient irrigation.[33]
- Real-time equipment maintenance[34]
- Aerial monitoring to detect changes in crop conditions[35]
- Thermal sensors can identify sick livestock by body temperature[36]

I. Improving Interoperability and Access

Many of the devices described above can bring benefits to more than one type of user or fulfill more than one purpose. For example, voice-enabled assistants such as the Amazon Echo can assist people who are visually impaired, but can also be useful for the elderly, or for people with injuries or other physical or mobility-related limitations.

Ultimately, promoting a more inclusive Internet may require using a significant amount of personal data and will almost certainly benefit from

[30] *See Smart Meters*, SMART GRID CONSUMER COLLABERATION, http://www.whatissmartgr*id*.org/smart-grid-101/smart-meters [https://perma.cc/X8P7-NCYH] (last visited Apr. 19, 2017).

[31] Pat Wilson & Stephanie Pow, *Financial Inclusion and the Internet of Things: How Smart Machines Can Benefit the Poor*, NEXT BILLION (Aug. 4, 2014), http://nextbillion.net/financial-inclusion-and-the-internet-of-things/ [https://perma.cc/H5MW-RVZ4].

[32] Christopher Long, *Internet of Things Not Just for Cities*, NEXT BILLION (Nov. 10, 2015), http://www.govtech.com/fs/internet/Internet-of-Things-Not-Just-for-Cities.html [https://perma.cc/R62H-7DL2].

[33] *Id.*

[34] *Id.* ("[S]ensors embedded in equipment transmit real-time data and alert farmers to any needed maintenance before a breakdown occurs.").

[35] *Id.* ("Drones with optical and multi-spectral sensors allow farmers to gather vast amounts of data and remotely monitor the health of their crops. Using this data, farmers can easily assess crop conditions using the Normalized Difference Vegetation Index (NDVI), which has its roots in the space program and measures variances in vegetation.").

[36] *Id.*

cloud-based infrastructure. For example, Raising the Floor, a consortium of academic, industry, and non-governmental organizations and individuals, has created the Global Public Inclusive Infrastructure (GPII) Project.[37] "GPII is a software and service enhancement to existing broadband infrastructure designed to . . . improve the interoperability" of assistive technologies by building in "ubiquitous accessibility" features.[38] The system is designed to provide a means for an individual to express accurate and current information about their needs and preferences in a given context and in a common language that can be understood by technical systems and services.[39] Such a storage system for private preferences and permissions would necessarily require significant data collection,[40] but nonetheless holds tremendous promise for expanding Internet accessibility.

IV. Emerging Industry Standards and Norms

Many of the assistive IoT technologies described above involve connected devices that are worn on the body, like the OrCam or the Dot (Braille smart watch), or comprise elements of an "always ready" Smart Home, like the Amazon Echo or the Google Home. These sub-categories of connected devices are illustrative of the benefits of assistive technology as well as the challenges of regulating IoT to protect consumer privacy.

A. Wearables

Wearable devices, which include fitness trackers, glasses, jewelry, clothing, and other body-worn items incorporating sensors and technology, and their related apps and services ("Wearables") help users track physiological information and hold the potential to improve lives.[41] Wearables deploy sensors to collect environmental, behavioral, and social data for and from their users.[42] Consumer-generated data from these devices is already creating substantial benefits for users by helping individuals manage their fitness, exercise, and biofeedback, improving personal

[37] *About the Global Public Inclusive Infrastructure (GPII)*, GLOBAL PUB. INCLUSIVE INFRASTRUCTURE, http://gpii.net/About.html [https://perma.cc/2PFF-Z4F6] (last accessed Mar. 2, 2017).

[38] *Id.*

[39] *See id.*

[40] *Private Preference & Permission System*, GLOBAL PUB. INCLUSIVE INFRASTRUCTURE, http://gpii.net/programs/private-preference-permission-system [https://perma.cc/7UEQ-2DQ7] (last visited Mar. 2, 2017).

[41] *See generally* FUTURE OF PRIVACY FORUM, BEST PRACTICES FOR CONSUMER WEARABLES AND WELLNESS APPS & DEVICES 1–3 (Aug. 2016), https://fpf.org/wp-content/uploads/2016/08/FPF-Best-Practices-for-Wearables-and-Wellness-Apps-and-Devices-Final.pdf [https://perma.cc/ELZ5-KR2A]; Janice Phaik Lin Goh, *Privacy, Security, and Wearable Technology*, LANDSLIDE, Nov.–Dec. 2015, https://www.americanbar.org/content/dam/aba/publications/landslide/2015-november-december/ABA_LAND_v008n02_privacy_security_and_wearable_technology.authcheckdam.pdf [https://perma.cc/VM2F-UQU7].

[42] *Id.*

productivity and efficiency, and making other technologies simpler and easier to use. Research based on data collected by Wearables could reveal insights that lead to early detection of medical conditions and other broad societal benefits.

If the data collected by Wearables is not properly protected or if used in unethical or illegal ways, individuals' privacy could be at risk. Critics worry that users could find themselves unfairly 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.[43]

Given the potential benefits that Wearables and consumer-generated wellness data may provide to consumers and society, it is important that this data be subject to privacy controls and used responsibly. Many leading Wearables providers and mobile application (app) developers have already set clear parameters for the collection and use of consumer-generated wellness data.[44] Platforms and devices that enable third-party apps or services to access data have also set forward terms for how those apps or services may use data collected via those devices or platforms.[45]

In many areas, data collected by Wearables is already subject to legal protections. In the United States, these protections include sector-specific regulations such as Children's Online Privacy Protection Act (COPPA), Federal Credit Reporting Act (FCRA), or the Americans with Disabilities Act (ADA), as well as federal and state laws governing insurance and illegal discrimination.[46] In many cases, personal wellness information is covered by Health Insurance Portability and Accountability Act (HIPAA), which imposes certain privacy and security requirements on healthcare providers and their business associates.[47] Medical devices that can be worn or carried like a consumer Wearable are also regulated for safety by the Food and Drug Administration (FDA).[48]

[43] Patience Haggin, *As Wearables in Workplace Spread, So Do Legal Concerns*, WALL ST. J. (Mar 13, 2016, 10:12 PM ET), https://www.wsj.com/articles/as-wearables-in-workplace-spread-so-do-legal-concerns-1457921550?mg=prod/accounts-wsj&mg=prod/accounts-wsj [https://perma.cc/ACW7-46TW].

[44] *See, e.g.*, *CDT and Fitbit Report on Best Privacy Practices for R&D in the Wearables Industry*, CTR. FOR DEMOCRACY & TECH. (May 18, 2016), https://cdt.org/insight/cdt-fitbit-report-privacy-practices-rd-wearables-industry/ [https://perma.cc/TDV4-CJPF].

[45] *See, e.g.*, *Healthkit*, APPLE, https://developer.apple.com/documentation/healthkit [https://perma.cc/VW2W-SM7M] (last visited Aug. 7, 2017).

[46] *See, e.g.*, *FPF List of Federal Anti-Discrimination Laws*, FUTURE PRIVACY F. (May 21, 2014), https://fpf.org/2014/05/21/fpf-list-federal-anti-discrimination-laws/ [https://perma.cc/E685-MXS4].

[47] *See generally* Kristen Lee, "Wearable Health Technology and HIPPA: What Is and Isn't Covered," TECHTARGET (last visited July, 30 2017, 11:26 PM ET), http://searchhealthit.techtarget.com/feature/Wearable-health-technology-and-HIPAA-What-is-and-isnt-covered [https://perma.cc/CHU8-7ZXT].

[48] *See generally What is a Medical Device?*, U.S. FOOD & DRUG ADMIN., https://www.fda.gov/aboutfda/transparency/basics/ucm211822.htm [https://perma.cc/232F-BG7Z] (last visited July 30, 2017, 11:27 PM ET).

However, many Wearables collect data that is unlikely to be covered by specific sectoral protections. Sometimes this data will be of low sensitivity and of the sort that some users will share with friends or publicly. For example, consumers may feel more comfortable sharing fitness progress data, like how many miles or steps they have taken in a day, as well as broad demographic information like gender. Other times, the data can be of the sort that can reveal highly sensitive facts about users and is information users will expect to be treated confidentially. Depending on the type of app, the types of uses, and the types of controls, the same data may be subject to very different user expectations.[49] In many instances, user expectations for data uses by new apps and new services are still evolving as new benefits and new risks become apparent.

In Europe and other jurisdictions, national (and soon EU-wide) privacy laws set baseline privacy and security expectations. While such laws provide the starting point for data protection, they often also impose higher standards on personal information that is considered especially sensitive, such as health or financial data.[50] In some cases, consumer-generated wellness data is likely to fall within such protected categories. The European Data Protection Supervisor, for example, has noted that:

> "Lifestyle and well-being data will, in general, be considered [sensitive] health data, when they are processed in a medical context…or where information regarding an individual's health may reasonably be inferred from the data (in itself, or combined with other information), especially when the purpose of the application is to monitor the health or well-being of the individual (whether in a medical context or otherwise)."[51]

Where lifestyle or wellness data *is* considered sensitive, additional restrictions on data processing are imposed. As the Article 29 Working Party has noted, however, "on the other side of the spectrum . . . there is a

[49] *See, e.g.*, Rosie Spinks, *Using a fitness app taught me the scary truth about why privacy settings are a feminist issue*, QUARTZ (Aug. 01, 2017), https://qz.com/1042852/using-a-fitness-app-taught-me-the-scary-truth-about-why-privacy-settings-are-a-feminist-issue/ [https://perma.cc/EGD7-L4R8].

[50] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), art. 9, 2016 O.J. (L 119), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679 [https://perma.cc/2N6Y-PQHP]. We also note that the recently published draft of the e-Privacy Regulation by the European Commission contains provisions related to the protection of "electronic communications data," and although it is still a draft, the Regulation could be interpreted broadly in coming years. *See Proposal for an ePrivacy Regulation*, EUR. COMMISSION, https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation [https://perma.cc/4JSX-2K4A] (last visited Mar. 2, 2017).

[51] Giovanni Buttarelli, *Opinion 1/2015 Mobile Health: Reconciling Technological Innovation with Data Protection*, EUR. DATA PROTECTION SUPERVISOR (May 21, 2015), https://edps.europa.eu/sites/edp/files/publication/15-05-21_mhealth_en_0.pdf [https://perma.cc/US9S-RLDQ].

category of personal data generated by lifestyle apps and devices that is, in general, not to be regarded as [sensitive] health data."[52] There are also some apps and devices where "it is not obvious at first sight whether or not the processing of these data should qualify as the processing of health data."[53]

It is important to distinguish between personal data that are, on the one hand, clearly akin to medical information which reveal inherently sensitive details about an individual's health status and, on the other hand, those raw or low-impact personal data that do not expose an individual's private health information. Given the lack of bright lines between sensitive health and non-sensitive lifestyle data, treating all health-related personal data the same would be a mistake. The stringent privacy, security, and safety requirements appropriate for medical devices and medical data would render many commercial fitness devices impractical for everyday consumers. At the same time, it would be a mistake to treat wellness data as if it were generic personal information without any sensitivity.

Rather, we should recognize that these data exist on a spectrum and that privacy protections and legal frameworks should be calibrated to the nature and sensitivity of the data, the social benefits from re-use of the data, controls exercised to protect against misuse of data, and consumers' evolving expectations. Where personal health or wellness data are inherently more sensitive, for example, their collection and use should be based on a narrower specification of purpose; additional consents should be required for each specified use; and all advertising should be based on express consent. But where data are less inherently concerned with health, a specified purpose might appropriately capture a *range* of tightly-related purposes, rather than requiring individualized notices for each and every compatible collection or use of wellness data, and advertising might be presented on an opt-*out* basis. For example, an app that captures a user's steps, height, and weight and whose purpose is to improve users' general fitness and wellness should be able to offer users the opportunity to consent to all compatible wellness or fitness uses of their data at once, rather than requiring additional notices and consents for every related purpose.

In determining where data fall on this spectrum, some relevant factors to consider would include: the context and purpose for which data are collected and used; whether data are inherently/clearly medical data; whether the data is made available to a member of the medical community; whether there is a clear and close link between the data and a user's health status; whether data is used to measure or predict health risks and/or to enable medical follow-up; whether conclusions are or can be reasonably drawn about the health status of a user based on the data; the compatibility of the use; and the existence of appropriate safeguards.[54] Practical guidance

[52] EUR. COMISSION, ARTICLE 29 WORKING PARTY, ANNEX–HEALTH DATA IN APPS AND DEVICES 3, http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf [https://perma.cc/6FAS-GY6F] (last visited July 30, 2017).

[53] *Id.*

[54] *See id.*

that can be further tailored to meet local requirements can build upon existing legal expectations. Apps and devices that capture other personally identifiable information should look to existing best practices and guidance documents, such as the FTC *Internet of Things Report*,[55] the Article 29 Working Party *Opinion on the Recent Developments on the Internet of Things*,[56] or the FPF-CDT *Best Practices for Mobile Application Developers*.[57]

B. "Always Ready" Home Devices

"Speech recognition—the ability to speak naturally and contextually with a computer system in order to execute commands or dictate language"[58]—has improved dramatically in recent years. Although the technology is far from perfect—the accuracy is diminished by background noise and recording quality, and certain accents are often more easily understood than others[59]—consumers in 2017 can now interact reasonably well via speech with a range of devices. This includes waking up and asking, "what's on my calendar?" to calibrating a connected thermostat, to dictating a text message or starting a browser search with the likes of "OK, Google," "Hey, Siri," "Hi Alexa," or "Hey, Cortana."

The benefits of speech recognition technology can be especially life-changing for people with disabilities, physical limitations, or visual impairments. Devices like the Amazon Echo, in part due to their affordability, provide a tool of independence even for routine tasks such as adjusting the lights, scheduling appointments, or ordering groceries.[60]

[55] FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [https://perma.cc/98AN-VMEU].

[56] Article 29 Protection Working Party, *Opinion 8/2014 on the Recent Developments on the Internet of Things*, EUR. COMMISSION (Sept. 16, 2014), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf [https://perma.cc/SK5L-U9FL].

[57] FUTURE OF PRIVACY FORUM & CTR. FOR DEMOCRACY & TECH., BEST PRACTICES FOR MOBILE APPLICATION DEVELOPERS (2011), https://www.cdt.org/files/pdfs/Best-Practices-Mobile-App-Developers.pdf [https://perma.cc/3KAP-DYY3].

[58] STACEY GRAY, FUTURE OF PRIVACY FORUM, ALWAYS ON: PRIVACY IMPLICATIONS OF MICROPHONE-ENABLED DEVICES 4 (2016), https://fpf.org/wp-content/uploads/2016/04/FPF_Always_On_WP.pdf [https://perma.cc/U87G-LEAH].

[59] Speech recognition expert Marsal Gavaldà calls this diminished accuracy for children, seniors, and people with accents "the speech divide." *See* Nora Young, *Here's Why Your Phone Can't Understand Your Accent*, CBC RADIO (Sept. 13, 2015), http://www.cbc.ca/radio/spark/292-what-you-say-will-be-searched-why-recognition-systems-don-t-recognize-accents-and-more-1.3211777/here-s-why-your-phone-can-t-understand-your-accent-1.3222569 [https://perma.cc/98FG-N7KG]; *see also* Daniela Hernandez, *How Voice Recognition Systems Discriminate Against People with Accents*, SPLINTER (Aug. 21, 2015, 7:00 am), http://fusion.net/story/181498/speech-recognition-ai-equality/ [https://perma.cc/K78Y-JH8P].

[60] *See* Allen St. John, *Amazon Echo Voice Commands Offer Big Benefits to Users with Disabilities*, CONSUMER REP. (Jan. 20, 2017),

A key feature is that by sending data to the cloud, where powerful computing can be applied, speech recognition services can improve over time.[61] Making use of the huge advancements in data processing in recent years, voice-to-text technologies can now adapt to your speech patterns over time and are getting better at understanding speech in context.[62] This aspect led early voice recognition pioneer Raj Reddy to predict that voice recognition technologies would pass the Turing Test in our lifetimes.[63]

"The same feature of speech recognition technology that makes it useful—its ability to bring voice control into our everyday lives—is the feature that is now understandably raising privacy concerns, as microphone-enabled devices become integrated into our homes and daily environments."[64] Speech activated "always ready" devices, such as the Amazon Echo or the Google Home, use the power of "energy efficient processors to remain in an inert state of passive processing for a pre-set 'wake phrase'."[65] "The device buffers and re-records locally, without transmitting or storing any information, until it detects the word or phrase that triggers the device to begin actively recording".[66] This key feature is critical to enabling greater digital access to people with disabilities or physical limitations: rather than requiring the user to manually turn the device on, or designing it transmitting data constantly, the device can be activated verbally such that it only transmits data when the user wants it to do so.

In contrast, other devices are designed to truly be "always on." "Always on devices are those designed to record and transmit data all of the time."[67] "Most prominently, this includes home security cameras and baby monitors but also includes a range of new devices."[68] "Cities can now detect gunfire via microphone networks and there are microphones that can detect termite infestations by listening to audio outside of the range of the human ear."[69] "These devices, because they are designed to be always on, evoke different privacy concerns from those that are manually or speech activated, and call for notice and consent frameworks in sync with the more extensive data collection that they enable."[70]

http://www.consumerreports.org/amazon/amazon-echo-voice-commands-offer-big-benefits-to-users-with-disabilities/ [https://perma.cc/5SWB-6QS9].

[61] *See generally* Xuedong Huang, James Baker & Raj Reddy, *A Historical Perspective of Speech Recognition*, COMM. ACM, Jan. 2014, at 94, http://cacm.acm.org/magazines/2014/1/170863-a-historical-perspective-of-speech-recognition/abstract [https://perma.cc/DW97-9BBM].

[62] *Id.*

[63] *Id.*

[64] GRAY, *supra* note 58.

[65] *Id. at 5.*

[66] *Id.*

[67] *Id.*

[68] *Id.*

[69] *Id.*

[70] *Id.* at 6.

"Microphones and specifically voice data retain unique social and legal significance."[71] "In some instances, laws that protect biometric information may apply."[72] "In general, sector-specific laws and regulations will also apply on the basis of the content of the voice communications."[73] "The collection of certain voice characteristics for the purpose of recognizing an individual, for example, implicates a range of laws".[74] "At the federal level, a 'voice print' is considered either a biometric or personal record in the context of the Privacy Act,[75] [Federal Educational Rights and Privacy Act (FERPA)],[76] and HIPAA,[77] and thus subjected to greater regulatory restrictions."[78] "Similarly, several states have expanded their legal definitions of personally identifiable information in certain identity theft or breach notification laws to include some form of biometrics."[79]

However, "the majority of speech-enabled devices on the market today are not designed for the purpose of uniquely identifying a person through the biometric characteristics of her voice."[80] "Instead, they aim to create products for which speech is a useful interface for engagement."[81] "In the future, however, it can be foreseen that unique voice recognition might become a useful consumer tool—for example, to permit only a specific person to access a device, or to enable parental controls by distinguishing between user accounts."[82] "Companies considering adding such features should be aware of the increasing number of federal and state laws regarding biometric identification."[83]

[71] *Id.*

[72] *Id.*

[73] *Id.*

[74] *Id.*

[75] 22 C.F.R. § 308.3 (2017) ("Record means any document, collection, or grouping of information about an individual maintained by the agency, including but not limited to . . . any other personal information which contains . . . a finger or voiceprint.").

[76] 34 C.F.R. § 99.3 (2017) ("Biometric record, as used in the definition of personally identifiable information, means a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual. Examples include . . . voiceprints.").

[77] 45 C.F.R. § 164.514 (2017) (listing "[b]iometric identifiers, including finger and voice prints" as examples of personal information that must be removed from a data set before that data set can be considered properly de-identified and thus no longer subject to HIPAA regulations).

[78] GRAY, *supra* note 58, at 6–7.

[79] *Id.*; *see, e.g.*, CONN. GEN. STAT. ANN. § 38a-999b (West 2017); IOWA CODE ANN. § 715C.1 (West 2017); NEB. REV. STAT. ANN. § 87–802 (West 2017); N.C. GEN. STAT. ANN. § 7566 (West 2017); OR. REV. STAT. ANN. §§ 165.800, 336.184 (West 2017) (regulating student educational records); WIS. STAT. ANN. § 943.201 (West 2017); WYO. STAT. ANN. § 6–3–901 (West 2017).

[80] GRAY, *supra* note 58, at 7.

[81] *Id.*

[82] *Id.*

[83] *Id.*; *see* 22 C.F.R. § 308.3 (2017) ("Record means any document, collection, or grouping of information about an individual maintained by the agency, including but not limited to . . . any other personal information which contains . . . a finger or voiceprint."); 34 C.F.R. § 99.3 (2017) ("Biometric record, as used in the definition of personally identifiable information means a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual. Examples include

"Moving forward it will be important to recognize that voice data is unique in its historical protection, communicative content, and biometric features."[84] "Useful guiding principles are beginning to emerge",[85] and companies can take many steps to build trust in these devices, including: (1) strong security measures, including encryption of data at rest and in transit; (2) hardware-level "on/off" switches, to address concerns about remote access; and (3) access to and ability to delete audio data.

Conversations will continue to evolve on this subject as social norms shift about when and where we should expect to be able to speak to our devices. In considering the benefits of speech-enabled devices in parallel to their legitimate privacy implications, forward-looking companies will be well-served to use the power of technology itself to enable the power of speech recognition while protecting consumer privacy and control.

V. CONCLUSION

When developing policies for IoT, policymakers must involve all stakeholders, including members of disability communities. Increasingly, privacy laws and regulations have an impact on assistive technologies, and policy discussions benefit from the involvement of those who are directly affected. For example, state laws restricting the collection of biometric identifiers might unintentionally hamper technologies that enable devices like the OrCam.[86] These devices and others—such as self-driving cars, cloud based screen readers, home monitoring systems, and many more—may rely on data-supported IoT technologies to deliver services.

Policymakers also need to allow for the fact that it will not always be practical to address the collection and use of personal information via traditional notice and choice mechanisms. Many connected devices will not have screens or interfaces that readily present privacy notices or allow consumers to select specific data practices. As a result, a flexible approach to the FIPPs will be needed. Many IoT devices are beginning to provide notice of data collection through visual, auditory, and tactile cues.[87]

. . . voiceprints"); 45 C.F.R. § 164.514 (2017) (listing "[b]iometric identifiers, including finger and voice prints" as examples of personal information that must be removed from a data set before that data set can be considered properly de-identified and thus no longer subject to HIPAA regulations).

[84] GRAY, *supra* note 58, at 10.

[85] *Id.*; LYNN TERWOERD ET AL., VOICE PRIVACY GUIDING PRINCIPLES, (2016), http://c.ymcdn.com/sites/www.ewf-usa.com/resource/collection/CAA076AF-9566-4E1E-9F07-6421154DE0EA/Voice_Privacy_Guiding_Principles_Public_(final).pdf [https://perma.cc/7WL5-6TNC].

[86] *E.g.*, 740 ILL. COMP. STAT. 14/1 to 14/99 (2017).

[87] The Amazon Echo, for example, uses a light ring to visually communicate its status. *See Alexa and Alexa Device FAQs*, AMAZON, http://www.amazon.com/gp/help/customer/display.html?nodeId=201602230 [https://perma.cc/Q7JM-Y22S] (last visited July 31, 2017). When the light is solid blue, the device is transmitting audio data. *See Id.* When all lights are off, the device is active and waiting for the user's request. *See Id.* Those who want to know more about the Echo's

Flexible and design-centered approaches such as these will help pave the way towards effective, consumer-protective policies for the Internet of Things. With the FIPPs as a guide to notice and consent frameworks, and a firm understanding of the nuances of the many devices entering the market, policymakers can protect consumer privacy while encouraging IoT as a tool for inclusion.

privacy policy can ask, "Alexa, are you spying on me?" and in response the device will state, "I only send audio back to Amazon when I hear you say the wake word. For more information and to view Amazon's privacy notice, visit the help section of your Alexa app." *See Id.*