The Internet of Things (IoT) and People with Disabilities: Exploring the Benefits, Challenges, and Privacy Tensions

January 2019

FUTURE OF PRIVACY FORUM

ABOUT THE FUTURE OF PRIVACY FORUM

The Future of Privacy Forum (FPF) is a catalyst for privacy leadership and scholarship, advancing responsible data practices in support of emerging technologies. FPF is based in Washington, DC, and includes an advisory board comprising leading figures from industry, academia, law, and advocacy groups.

Authors:
Lauren Smith, Policy Counsel, Future of Privacy Forum
Carson Martinez, Policy Fellow, Future of Privacy Forum
Chanda Marlowe, Christopher Wolf Diversity Fellow, Future of Privacy Forum
Henry Claypool, Senior Fellow, Future of Privacy Forum & Policy Director, Community Living Policy Center at the University of California, San Francisco

Research for this paper was supported by the Comcast Innovation Fund and conducted in consultation with the American Association of People with Disabilities (AAPD) Technology Forum and several other stakeholders. See Appendix I for the full list of stakeholders who provided feedback over the course of the drafting process.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Internet of Things (IoT) has the potential to transform the lives of people with disabilities,[1] industries, and society as a whole. Many of today's IoT devices and services are increasingly accessible to people with disabilities; some IoT technologies are specifically designed for people with disabilities, whereas others are repurposed by them.[2] The IoT and its associated data are producing accessibility-related advances, ranging from smart home devices to self-driving cars. IoT devices and services are also empowering people with disabilities to participate more fully and autonomously in everyday life by reducing some needs for human intermediaries or accommodations. Data derived from people with disabilities' use of IoT devices and services can provide insights into the challenges and opportunities experienced by users. These insights can enhance existing IoT products and lead to the development of new ones.

Despite the many potential benefits that IoT devices and services can provide to people with disabilities, the collection, use, and sharing of user data generated by these devices and services can raise unique privacy risks. Depending on the circumstances, IoT technologies can enhance or diminish privacy, creating possible tensions between privacy gains and losses. IoT privacy risks can be exacerbated for people with disabilities when privacy notices and controls fail to take into account the diversity of users' needs. How people address these risks depends on context, including how the service or device is used, who is using it, and individual preferences and values. Members of the disability community may weigh the benefits and privacy risks differently.

This consideration—weighing the ways in which IoT devices and services benefit people with disabilities but concurrently create privacy risks via data collection—deserves more nuanced consideration and engagement by stakeholders, including users, companies, advocates, policymakers, and others. This paper explores the unique privacy considerations that people with disabilities face when using IoT devices and services, specifically regarding transparency, individual control, respect for context, focused collection, and security. We also provide recommendations to address privacy risks.

Recommendations:

1. **Prioritize Inclusive Design**. Accessibility and the privacy of people with disabilities should not be an afterthought for the IoT and new technology developers—people with disabilities should be included in the design of IoT technologies. The appropriate timing for integrating accessibility is during the earliest possible stage of design.

2. **Promote Research and Innovation**. To successfully build the IoT with universal or accessible design, both qualitative and quantitative research is needed to better understand how people with disabilities use the IoT and feel about its current privacy landscape.

---

[1] The Americans with Disabilities Act (ADA) of 1990 defines a person with a disability as a "person who has a physical or mental impairment that substantially limits one or more major life activity." *Top ADA Frequently Asked Questions*, AMS. WITH DISABILITIES ACT NAT'L NETWORK, https://adata.org/top-ada-frequently-asked-questions (last visited Jan. 14, 2019). Other federal laws define a person with a disability as "[a]ny person who has a physical or mental impairment that substantially limits one or more major life activities; has a record of such impairment; or is regarded as having such an impairment." *Disability Overview*, U.S. DEP'T OF HOUS. AND URBAN DEV., https://www.hud.gov/program_offices/fair_housing_equal_opp/disability_overview, (last visited Jan. 14, 2019).

[2] *See infra* Appendices II (discussion) and III (chart) for a taxonomy of the IoT used by people with disabilities.

3. **Build Privacy-by-Design Approaches**. Companies not only should consider the sensitive nature of the data collected from the IoT used by people with disabilities and the diversity of users' needs (e.g., auditory, visual, or haptic), but also incorporate such considerations when developing privacy disclosures, notices, and other controls within IoT products.

4. **Foster Cross-Sector Collaborations**. Advocates, academia, policymakers, and industry should work together to adapt the use of the IoT for people with disabilities and develop IoT solutions that meet the current and anticipated needs of such people.

5. **Enhance Awareness of Data Risks and Benefits**. Policymakers should consider not only the potential enhanced risks that people with disabilities may face when using the IoT, but also the enhanced autonomy that these same technologies provide to disability communities. Members of the disability community should consider becoming engaged in policy processes and voicing their views on the privacy challenges that they face when using IoT devices and services.

INTRODUCTION

Today, an estimated 8.4 billion connected devices are in use worldwide.[3] While there are no statistics on how many people with disabilities use IoT devices and services,[4] the number is likely increasing rapidly due to the overall increase in uptake and everyday use of the IoT.[5] As the number of IoT devices and services available for and used by people with disabilities increases, stakeholders must engage in a substantive conversation about the privacy implications of such uses.

This white paper evolved out of discussions with stakeholders in 2017–2018, including two convenings that the Future of Privacy Forum (FPF) hosted with the American Association of People with Disabilities (AAPD) Technology Forum, with support from the Comcast Innovation Fund. These convenings brought together a diverse group of industry professionals, consumer organizations, disability advocates, and other thought leaders to discuss the opportunities that the IoT provide for people with disabilities, the data that may be generated and used by these devices and services, and the privacy challenges that may result. These discussions helped to advance conversations about inclusive IoT devices and services, illuminating the benefits and privacy concerns central to people with disabilities. See Appendix I for the full list of stakeholders who provided feedback over the course of the drafting process.

The IoT can benefit people with disabilities but can also create privacy challenges. Often, these challenges can be mitigated when they are discussed and addressed early on. By examining the issue through the lens of the Fair Information Practice Principles (FIPPs)—ranging from transparency, individual control, respect for context, focused collection, to security—we can better understand the unique privacy considerations and tensions that people with disabilities may face when using IoT devices and services. While the FIPPs apply to all users, close examination of them in this context can shed light on how IoT devices and services may uniquely affect people with disabilities.

This paper explores how stakeholders can protect individual privacy while increasing people with disabilities' access to IoT devices and services. **Part I** describes the benefits the IoT can offer to people with disabilities, societies, and companies, particularly regarding the collection, use, and sharing of data derived from people with disabilities' interaction with the IoT. **Part II** discusses the privacy impacts faced by people with disabilities who use IoT devices and services, examined through

---

[3] Press Release, Gartner, Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016 (February 7, 2017), https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016.

[4] According to a 2013 study, 92% of people with disabilities use a "wireless device such as a cell phone or tablet." *SUNspot —Use of Wireless Devices by People with Disabilities*, 1 WIRELESS REHABILITATION ENGINEERING RESEARCH CENTER (2013), www.wirelessrerc.org/sites/default/files/publications/sunspot_2013-01_wireless_devices_and_people_with_disabilities_final1.pdf. According to a 2015 survey, nearly 70% of approximately 2,500 screen users used screen readers on their mobile devices. Close to half (44% of respondents) indicated that they use mobile screen readers as much or more than they use desktop/laptop screen readers. Many of them use a screen reader, a piece of software that relays content and functions audibly to the user. *Screen Reader User Survey #6 Results*, WEB ACCESSIBILITY IN MIND (Aug. 28, 2015), http://webaim.org/projects/screenreadersurvey6/.

[5] News Release, Trustwave, New Trustwave Report Shows Disparity Between IoT Adoption and Cybersecurity Readiness, Trustwave (February 28, 2018), https://www.trustwave.com/Company/Newsroom/News/New-Trustwave-Report-Shows-Disparity-Between-IoT-Adoption-and-Cybersecurity-Readiness/; Allen St. John, *Amazon Echo Voice Commands Offer Big Benefits to Users With Disabilities*, CONSUMER REPS. (January 20, 2017), https://www.consumerreports.org/amazon/amazon-echo-voice-commands-offer-big-benefits-to-users-with-disabilities/.

the lens of the FIPPs. **Part III** provides recommendations that promote the privacy of people with disabilities, encourage innovation, and prioritize access and inclusion.

I. WHY FOCUS ON THE IOT FOR PEOPLE WITH DISABILITIES?

The Internet of Things refers to "an ecosystem in which applications and services are driven by data collected from devices that sense and interface with the physical world."[6] The list of connected devices is ever-expanding and ranges from items that offer greater convenience and improved lifestyles such as voice-activated assistants, health-monitoring devices, and personal fitness trackers, to random objects such as dental floss, hairbrushes, and toothbrushes, to name a few. Many papers have been written on the general promise and privacy implications of the IoT.[7] Far fewer have addressed the privacy implications of the IoT specific to its use by people with disabilities.[8] An estimated 15% of the world's population lives with some sort of disability,[9] and their needs and desires call for greater exploration. The potential benefits of building IoT devices and services for people with disabilities are far-reaching:[10]

For people with disabilities**,** the IoT can be transformational because it can enhance safety, mobility, and independence—which can often lead to enhanced privacy. From internet-connected prosthetics to smart shoes that vibrate to guide the wearer in the right direction, many IoT devices and services have been designed to enhance the lives of people with disabilities and reduce their dependence on others. A few examples:

- For people with developmental disabilities, reminder apps such as My PillBox[11] help users to identify and take medications at the right time each day, thus enhancing their safety.

---

[6] Eur. Comm'n, Working Party on Commc'n Infrastructures & Servs. Policy, The Internet of Things: Seizing the Benefits and Addressing the Challenges (2016), http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/CISP(2015)3/FINAL&docLanguage=En.

[7] *See*, *e.g.*, Adam D. Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation*, 21 RICH. J.L. & TECH 6 (2015), https://scholarship.richmond.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1409&context=jolt; Xavier Caron, Rachelle Bosua, Sean Maynard, & Atif Ahmed, *The Internet of Things (IoT) and its Impact on Individual Privacy: An Australian Perspective*, 32 COMPUTER L. & SECURITY REV. 1 (2016), http://daneshyari.com/article/preview/465454.pdf.

[8] *See*, *e.g.*, Jillisa Bronfman, *Weathering the Nest: Privacy Implications of Home Monitoring for the Aging American Population*, 14 DUKE L. & TECH. REV. 192 (2016) (focusing primarily on the elderly population rather than a broad range of disabilities); Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85 (2014) (focusing on racial and economic discrimination rather than a broad range of disabilities), http://scholar.law.colorado.edu/articles/83.

[9] According to the World Health Organization, 360 million people have moderate to profound hearing loss, 285 million people have visual disabilities (39 million of whom are blind), and 75 million people need a wheelchair. WORLD HEALTH ORGANIZATION & WORLD BANK, WORLD REPORT ON DISABILITY (2011), http://apps.who.int/iris/bitstream/10665/70670/1/WHO_NMH_VIP_11.01_eng.pdf.

[10] In past papers, we have discussed how the IoT can provide tools of inclusion by highlighting specific examples in which IoT devices and services can improve the day-to-day quality of life of people with disabilities. Jules Polonetsky & Stacey Gray, *The Internet of Things as a Tool for Inclusion and Equality*, 69 FED. COMM. L. J. 103, http://www.fclj.org/wp-content/uploads/2017/10/69.2.1-Polonetsky-et-al.pdf. This paper will discuss the benefits and challenges of data collection, use, and sharing via IoT devices and services accessible to or used by people with disabilities, which range from improved policymaking to better devices.

[11] MY PILLBOX, https://www.mypillbox.org/ (last visited Jan. 14, 2019).

- For people who are blind or have visual disabilities, products such as OrCam[12] and Aira Smart Glasses[13] enable users to navigate their surroundings and access written information, thus enhancing their mobility and autonomy.
- For people with physical disabilities, smart home technology such as Nest[14] allows users to control items in their homes that may be physically difficult to reach, such as lights, door locks, or security systems, thus enhancing their independence. This technology also allows people with visual disabilities to control and receive information from appliances such as thermostats, which are not always accessible.

In addition to those benefits, accessible IoT devices and services open the door for collecting more data about people with disabilities, which can create both benefits and challenges. One benefit can include filling gaps in the "data divide," i.e., the lack of high-quality data about certain individuals or communities.[15] Mitigating the data divide could improve policymaking and allocation of resources, lead to better products and services for people with disabilities,[16] and ultimately help to reduce social and economic inequalities.[17]

For society, universal design and accessible design have improved accessibility. Universal design is "the practice of designing products, buildings and public spaces and programs to be usable by the greatest number of people," and accessible design is "a design process in which the needs of people with disabilities are specifically considered."[18] From closed-captioning technologies to virtual assistants, universal and accessible design of the IoT can enhance the lives of everyone, not just people with disabilities. Today, many of the auto-complete and voice-recognition technologies that the general public enjoy started out as features designed to help people with disabilities use computers. This principle—whereby society benefits from laws, programs, and technologies designed to benefit vulnerable groups—was coined the "curb-cut effect," after curb cuts made walking the streets more bearable for everyone (e.g., parents pushing strollers, shoppers carrying groceries, etc.), even though the cuts were originally intended for wheelchair users.

When accessible technologies are created, society also benefits from the inclusion of people with disabilities. For example, consider Facebook's facial recognition feature. The feature, which can be used by all Facebook users to tag images, help combat fake accounts, and alert users when they

---

[12] OR CAM, http://www.orcam.com/ (last visited Jan. 14, 2019).

[13] AIRA, https://aira.io/ (last visited Jan. 14, 2019).

[14] NEST, https://nest.com/app (last visited Jan. 14, 2019); INTERNET OF THINGS: NEW PROMISES FOR PERSONS WITH DISABILITIES, GLOB. INITIATIVE FOR INCLUSIVE INFOR. & COMMC'N TECHS, (July 2015), http://www.g3ict.org/press/press_releases/press_release/p/id_89.

[15] Daniel Castro, Center for Data Innovation, The Rise of Data Poverty (2014), http://www2.datainnovation.org/2014-data-poverty.pdf.

[16] For instance, sensors in prosthetics can track how the user performs with the device, and this information can lead to the development of newer models. Those newer models can provide more options to best cater to how the person uses the prosthetic. Also, the sensors can track how the individual maneuvers around their house, and that data could translate to better accessibility methods to improve their way of life.

[17] Daniel Castro, Center for Data Innovation, The Rise of Data Poverty (2014), http://www2.datainnovation.org/2014-data-poverty.pdf.

[18] *What is the Difference Between Accessible, Usable, and Universal Design?,* THE DISABILITIES, OPPORTUNITIES, INTERNETWORKING, AND TECHNOLOGY CENTER (Sept. 15, 2017), https://www.washington.edu/doit/what-difference-between-accessible-usable-and-universal-design (last visited Jan. 14, 2019).

have been recognized in a photo or video,[19] also allows people with visual disabilities to identify their friends in photos or videos. Inclusive participation (both in online and offline spaces) benefits society by creating a more diverse environment that fosters engagement and provokes creativity.[20] In the future, the same artificial intelligence (AI) technology that helps blind users search photos may be integral to the field of robotics. As characterized by the *Fast Company* article "How Designing For Disabled People is Giving Google An Edge," "the robots of the future might be able to 'see' because of the accessibility work done in computer vision for blind people today."[21]

For companies, numerous economic benefits can result from designing IoT products and services for people with disabilities. One obvious benefit is the ability to gain more customers. There is the potential to tap into the global elderly and disability assistive-devices market, which was valued at $14 billion in 2015 and is expected to surpass $26 billion by 2024.[22] There are also opportunities to reach new customers without disabilities, as many IoT products and services designed for people with disabilities rise to mainstream popularity.[23]

Companies may also benefit from cost savings. While designing for accessibility may seem to cost more at the outset, incorporating accessibility at the start of product development is significantly easier and less expensive than making improvements to a device or service after it has been rolled out. In 2017, McDonald's, Kmart, and Grubhub were among the growing number of websites that settled cases alleging that their websites and mobile applications were not accessible to the blind.[24] Companies that design and produce the IoT must also consider the potential economic cost of legal actions or reputational harm. As stated by Microsoft's Accessibility, Sustainability, and Environment Policy lead, Adina Braha-Honciuc, "[Designing] for accessibility [is] not just the nice thing to do, but the smart thing to do."[25]

---

[19] Joaquin Quiñonero Candela, *Managing Your Identity on Facebook with Face Recognition Technology*, FACEBOOK NEWSROOM (Dec. 9, 2017), https://newsroom.fb.com/news/2017/12/managing-your-identity-on-facebook-with-face-recognition-technology/.

[20] Katherine W. Phillips, *How Diversity Makes Us Smarter*, SCIENTIFIC AMERICAN (Oct. 1, 2014), https://www.scientificamerican.com/article/how-diversity-makes-us-smarter/.

[21] John Brownlee, *How Designing for Disabled People is Giving Google an Edge*, FAST COMPANY (May 23, 2016), https://www.fastcodesign.com/3060090/how-designing-for-the-disabled-is-giving-google-an-edge.

[22] T.J. McCue, *Elderly and Disabled Assistive Technology to Surpass $26 Billion by 2024*, FORBES (Mar. 21, 2017), https://www.forbes.com/sites/tjmccue/2017/03/21/elderly-and-disabled-assistive-technology-market-to-surpass-26-billion-by-2024/#61e2bf5269ea.

[23] Andrew Jack, *Disability Tech Goes Mainstream*, FINANCIAL TIMES (Oct. 26, 2017), https://www.ft.com/content/ae91d600-8caf-11e7-9580-c651950d3672.

[24] Each lawsuit claimed that failure to make these accommodations is a violation of the Americans with Disabilities Act. Samantha Bomkamp, *McDonald's, Kmart, Others Settle Suits Over Website Access for the Blind*, CHICAGO TRIBUNE (Nov. 29, 2018), http://www.chicagotribune.com/business/ct-biz-blind-website-settlements-20171107-story.html; Charles Marion, *ADA Website Accessibility Lawsuits on the Rise: Companies Should Review Their Potential Exposure*, JD SUPRA (Apr. 20, 2018), https://www.jdsupra.com/legalnews/ada-website-accessibility-lawsuits-on-16925/; Frank Morris, *Will Apps Become the Next Disability Lawsuit Target*, TECHCRUNCH (2015), https://techcrunch.com/2016/03/20/will-apps-become-the-next-disability-lawsuit-target/.

[25] Adina Braha-Honciuc, *Accessibility in the Workplace – a Competitive Edge*, MICROSOFT EU POLICY BLOG (June 28, 2016), https://blogs.microsoft.com/eupolicy/2016/06/28/accessibility-in-the-workplace-a-competitive-edge/ (last visited Jan 14, 2019).

II. The Unique Privacy Considerations of People with Disabilities

While data derived from people with disabilities' use of IoT devices and services can provide insight into their situations, the collection, retention, and sharing of vast amounts of such data also introduces potential privacy risks. The United Nations (UN) Convention on the Rights of People with Disabilities (CRPD) Article 22 has acknowledged the importance of privacy for people with disabilities:

> No person with disabilities, regardless of place of residence or living arrangements, shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence or other types of communication or to unlawful attacks on his or her honour and reputation. Persons with disabilities have the right to the protection of the law against such interference or attacks. States Parties shall protect the privacy of personal, health and rehabilitation information of persons with disabilities on an equal basis with others.[26]

Currently, 177 countries have ratified the convention.[27] While other governing bodies have acknowledged that such a right to privacy exists for people with disabilities, how this right manifests has yet to be deeply examined. As technologies and connected devices become common in everyday life, many questions and issues have arisen concerning how these devices affect the privacy of people with disabilities. IoT devices and services have the capacity for granular and ubiquitous data collection, which not only opens the door to new and important benefits but also to significant privacy risks.[28] While the IoT is still evolving, it is essential to identify the privacy tensions that people with disabilities face when interacting with IoT devices and services, to enable their equal participation in technological progress.

People with disabilities and other vulnerable populations may have distinct privacy expectations from those of the general population. As explained by Louis Brandeis and Samuel Warren in their 1890 articulation of legal privacy, the right "to be let alone" is of little use to those whose economic circumstances necessitate a life of interdependence; "the common law principle that a 'home is man's castle,' is worthless if you don't have a home."[29] The same could be said of interdependence due not only to economic circumstance but also to disability. Many people with disabilities require the accommodation of caregivers, teletypewriter (TTY) or video relay service (VRS) intermediaries, interpreters, or other aides to help them in their daily lives. This reliance on others in daily life can produce differing baseline privacy expectations for people with disabilities, both in terms of how much they must share or expose in order to receive such accommodation and what they expect from assistants.

In many ways, IoT devices and services allow people with disabilities to keep more information about their everyday lives confidential, by allowing them to perform more activities without the need for human intermediaries. For example, for deaf or hard-of-hearing people who require intermediaries or

---

[26] United Nations Gen. Assembly, Convention on the Rights of Persons with Disabilities and Optional Protocol (2007), A/RES/61/106. http://www.un.org/disabilities/documents/convention/convoptprot-e.pdf.

[27] *Convention on the Rights of Persons with Disabilities (CRPD)*. United Nations Dep't of Econ. and Soc. Affairs, https://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities.html (last visited Jan 29, 2019). (The United States has not ratified the CRPD).

[28] Edith Ramirez, FTC Chairman, Fed. Trade Comm'n, Opening Remarks, Privacy and the IoT: Navigating Policy Issues International Consumer Electronics Show (Jan. 6. 2015), http://www.ftc.gov/system/files/documents/public_statements/617191/150106cesspeech.pdf.

[29] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).

others to help them participate in everyday life, IoT devices and services such as Wavio[30]—a sound-capturing unit that can be programmed to hear various sounds, ranging from a baby's cry to a fire alarm, and send an alert to the user's device—can help maintain their independence by allowing them to live alone, thereby enhancing their privacy. By decreasing the need for human intermediation, the IoT can offer many such modes of confidentiality not previously available to people with disabilities.[31]

Although these technologies can diminish dependence on others, IoT developers may gain access to data produced through the use of devices or services. IoT devices and services may create new channels for independent mobility, communication, and other activities, but some devices and services may also create privacy risks. IoT devices and services may be data-intensive and -dependent, potentially revealing detailed private information about users and producing privacy risks.

As described by Ben Wittes and Jodie C. Liu in *The Privacy Paradox: The Privacy Benefits of Privacy Threats*, technology, including the IoT, can create tensions between privacy gains and privacy losses for all users. How people balance those tensions typically depends on context—how the IoT is used, who is using it, and what sorts of privacy people value.[32] For the disability community, the tabulation of privacy gains and losses differs from that of other communities. Some research has suggested that when older adults must choose among privacy, safety, independence, or mobility, they may be most willing to give up privacy protections.[33] Some people with disabilities may wish to make similar tradeoffs. Other studies have shown that elderly people judge technologies in terms of immediate benefit, and privacy may come second to other pressing needs.[34] Further, research has shown that the greater the perceived needs, the more willing people with disabilities are to share information or give up privacy.[35] Overall, these findings suggest that people may be willing to accept collection and

---

[30] *Wavio*, DEAF PEOPLE AND TECHNOLOGY COMPENDIUM, https://deaftechcompendium.wordpress.com/2017/05/09/wavio/ (last visited Jan. 14, 2019).

[31] For example, the use of smart speakers to purchase products online can enhance the privacy of people with disabilities by allowing people with mobility or visual disabilities to decrease their reliance on family members, friends, or other intermediaries to purchase those products for them.

[32] BENJAMIN WITTES & JODIE C. LIU, THE PRIVACY PARADOX: THE PRIVACY BENEFITS OF PRIVACY THREATS, BROOKINGS CENTER FOR TECH. INNOVATION (2015), https://www.brookings.edu/wp-content/uploads/2016/06/Wittes-and-Liu_Privacy-paradox_v10.pdf.

[33] Anita Melander-Wikman et al., *Safety vs. Privacy: Elderly Persons' Experiences of a Mobile Safety Alarm*, HEALTH & SOC. CARE IN THE COMMUNITY (2008), https://www.ncbi.nlm.nih.gov/pubmed/18613909; S.J. Brownsell et al., *Do Community Alarm Users Want Telecare?*. J. OF TELEMEDICINE & TELECARE (2000), https://journals.sagepub.com/doi/10.1258/1357633001935356/; G. Demiris & B.K .Hensel, *Technologies for an Aging Society: A Systematic Review of "Smart Home" Applications*, Y.B. MED. INFO. (2008), https://www.ncbi.nlm.nih.gov/pubmed/18660873; *WC Mann, et al., Elder Acceptance of Health Monitoring Devices in the Home,* 3 CARE MANAGEMENT JS. 91–98 (2002), https://www.ncbi.nlm.nih.gov/pubmed/12455220; Annie-Sophie Melenhorst et al., *Potential Intrusiveness of Aware Home Technology: Perceptions of Older Adults*, HFES 48TH ANN. MEETING (2004); K.E. Caine et al., *Benefits and Privacy Concerns of a Home Equipped with a Visual Sensing System: A Perspective from Older Adults*, PROC. OF THE HUM. FACTORS & ERGONOMICS SOC., 50TH ANN. MEETING 180-184 (2006); Scott Beach et al., *Disability, Age, and Informational Privacy Attitudes in Quality of Life Technology Applications: Results from a National Web Survey*, 5 ACM TRANSACTIONS ON ACCESSIBLE COMPUTING 2 (2009), http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.607.4935&rep=rep1&type=pdf.

[34] L. Magnusson & E.J. Hanson, *Ethical Issues Arising from a Research, Technology and Development Project to Support Frail Older People and their Family Careers at Home*, 11 HEALTH & SOC. CARE IN THE COMMUNITY 431–439 (2003), https://www.ncbi.nlm.nih.gov/pubmed/14498840.

[35] Scott Beach, *Disability, Age, and Informational Privacy Attitudes in Quality of Life Technology*, 5 ACM TRANSACTIONS ON ACCESSIBLE *Computing* (2009), http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.607.4935&rep=rep1&type=pdf,

use of their data when the result is greater independence or security of their person or property.

A. THE FAIR INFORMATION PRACTICE PRINCIPLES AS CONTEXT

The Fair Information Practice Principles (FIPPs) are internationally recognized principles that have long provided the foundation for consumer privacy protection. Over time, as technologies and the global privacy context have changed, the FIPPs have been presented with different emphases.[36] At their core, the FIPPs articulate basic protections for handling personal data and serve as a common language of privacy and a basis for law, regulation, and international agreements, including most recently the European Union's General Data Protection Regulation. These high-level guidelines were first articulated in 1973 by the United States Department of Health, Education, and Welfare's Advisory Committee on Automated Personal Data Systems. The Advisory Committee issued its report, *Records, Computers and the Rights of Citizens,* and called on Congress to adopt a "Code of Fair Information Practices," based on five principles.[37] These five principles formed the basis of subsequent codes and laws related to information collection, including the United States Privacy Act of 1974. In 1980, the Organizations for Economic Cooperation and Development adopted principles based on the US Code of Fair Information Practices, comprising eight principles to harmonize national privacy legislation without interfering with transborder information flows.[38] In 2012, the Obama Administration published the Consumer Privacy Bill of Rights, which builds on the FIPPs and consists of seven principles that serve as a baseline of privacy protections for consumers.[39]

The FIPPs continue to evolve, and their implementation has been carried out statutorily, regulatorily, and voluntarily by companies themselves. Implementation varies widely depending on the country,

---

[36] *See* ROBERT GELLMAN, FAIR INFORMATION PRACTICES: A BASIC HISTORY (2017), HTTPS://BOBGELLMAN.COM/RG-DOCS/RG-FIPSHISTORY.PDF.

[37] U.S. DEP'T. OF HEALTH, EDUC. & WELFARE, REPORT OF THE SECRETARY ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, RECORDS, COMPUTER, & THE RIGHTS OF CITIZENS (1973), https://www.justice.gov/opcl/docs/rec-com-rights.pdf. The five principles are as follows:

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for a person to find out what information about the person is in a record and how it is used.
3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
4. There must be a way for a person to correct or amend a record of identifiable information about the person.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.

[38] ORGANISATION FOR ECONOMIC CO-OPERATION & DEVELOPMENT, OECD GUIDELINES ON THE PROTECTIONS OF PRIVACY & TRANSBORDER FLOWS OF PERSONAL DATA (2013), http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Principles include (1) Collection Limitation, (2) Data Quality, (3) Purpose Specification, (4) Use Limitation, (5) Security Safeguards, (6) Openness (7) Individual Participation, (8) Accountability. In 2013, the OECD issued updated guidelines to replace the original 1980 guidelines. ORG. FOR ECON. CO-OPERATION & DEV., RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (2013), https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.

[39] THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY, 4 J. OF PRIVACY & CONFIDENTIALITY 2, 95-142. (2012), http://repository.cmu.edu/cgi/viewcontent.cgi?article=1096&context=jpc. Principles include (1) Transparency, (2) Individual Control, (3) Respect for Context, (4) Security, (5) Focused Collection, (6) Access and Accuracy, and (7) Accountability.

the company, the type of data, and many other factors. Regardless of their particular implementation, the FIPPs provide a common architecture of the rights and responsibilities concerning the collection and use of personal data.

Through the lens of the FIPPs, we can better understand the unique privacy considerations and tensions that people with disabilities may face when using IoT devices and services. While FIPPs apply to all users, a close examination of their individual implications can shed light on how IoT devices and services may uniquely impact people with disabilities. For example, many users depend on cloud technologies daily, thus producing a general privacy interest in the data collected from such products.

Below we outline some of the FIPPs that may require unique consideration in the context of people with disabilities' interaction with IoT devices and services: transparency, individual control, security, focused collection, and respect for context (see Table 1 on page 16).[40] We divide these unique privacy considerations into two separate categories: (1) the use of the IoT *by* people with disabilities and (2) the collection, sharing, and use of IoT data *about* people with disabilities.

1. Privacy Considerations: The Use of the IoT *by* People with Disabilities

Transparency

Under the FIPPs framework, users have a right to easily understandable and accessible information about privacy and security practices. Traditionally, transparency has been implemented in IoT devices and services through privacy policies and features within or on devices to notify users when data are collected (or not). Transparency mechanisms, however, can pose unique challenges for people with disabilities. Attempts to address transparency in IoT devices and services often fail to account for the unique accessibility needs of people with disabilities, who are thus often left out when consent is obtained or notice is provided about data collection.

It is vital that companies building notice mechanisms consider, from the outset of a product's design, the diversity of users' needs. For example, Amazon Alexa devices use a light ring to visually indicate when the device is collecting audio data. When the light ring is solid blue, the device is listening. When all lights are off, the device is active and waiting for a request. The solid red light indicates that the user has turned off the microphones on the device.[41] Addressing transparency exclusively via light cues could prevent people with visual disabilities from knowing when or whether data are being collected. Without an auditory or haptic interface, people who are blind or have visual disabilities are excluded from understanding when data are being collected about them. Amazon Alexa devices now also have a setting that allows users to enable auditory cues as an alternative, including a "start of request sound," which plays a short audible tone after the "wake" word has been recognized, to indicate that the devices are listening and streaming audio to the cloud, as well as an "end of request sound," which indicates that the connection has closed and the device is no longer streaming audio.[42]

With regard to consent, for example, smart home devices that connect with various other devices in

[40] Other FIPPs, such as Access and Accuracy and Accountability, while vital for the protection of personal information of all users, do not reveal any unique privacy considerations for the disability community when interacting with IoT devices and services.

[41] *Alexa and Alexa Device FAQs*, AMAZON, http://www.amazon.com/gp/help/customer/display.html?nodeId=201602230 (last visited Jan. 14, 2018).

[42] However, the "start of request sound" and "end of request sound" are not a default mechanism and must be manually turned on through the associated app.

the home or with an app may require users to agree to data sharing between such devices. This agreement can be completed via click-through consent mechanisms. To agree to data sharing between products, people with visual disabilities may require large-print documents or screen-reader applications, which may be incompatible with IoT devices and services. As products become increasingly interconnected, consent mechanisms need to include accessible designs or allow for interoperability with outside accessible technologies and software, so that users can access consent mechanisms.

For some people with developmental disabilities, providing meaningful consent can be challenging, as many privacy policies and consents are written at an eighth-grade reading level or higher, which may not accommodate the users' comprehension levels.[43] Images and easy-to-read summaries of key privacy practices could help mitigate this issue. Many IoT devices and services are beginning to provide notice and consent of data collection through visual, auditory, or haptic cues.[44] Technologies must continue to integrate such options, given that sufficient notice and consent may require implementing various tactics and options to ensure that the disability community's broad array of needs are addressed.

Individual Control

Perhaps one of the most significant barriers to the disability community's ability to take full advantage of the IoT involves choice and control. According to the FIPPs, the principle of individual control requires that companies provide users the right to control the personal data that companies collect from them and how they use it. However, for people with disabilities using IoT devices or services, expressing such control can be challenging. These challenges can manifest through two scenarios: (1) an individual's ability to choose *among* IoT devices and services and (2) an individual's ability to select data-collection settings *within* IoT devices and services.

Choices Among IoT Devices and Services

In general, individual control in IoT devices and services occurs through the ability to choose among different products that offer varying levels of data collection or choice. Because people with disabilities often are not considered in the design of new IoT products, such people are continually limited in their individual control of IoT devices and services. To maximize products, companies may attempt to produce devices with the lowest production costs, making it easy to ignore or cut out additional design features that promote accessibility. Companies may build IoT devices or services with proprietary applications or block accessibility apps or add-ons, preventing people with disabilities, who need to use apps on top of the IoT, from easily using such devices. However, companies that do not build accessibility into devices from the start must absorb the future costs of rebuilding or retrofitting the product in an accessible manner.

For people with disabilities, when IoT devices or services are not accessible, this restricts the types of products available to them and decreases their options. Limited choices in the actual devices translates to few ways to exercise control. For instance, when searching for a new smartwatch, people with visual disabilities may be limited in the number of devices from which to choose, because

---

[43] Another related challenge that many industries face is how to make privacy risks and policy considerations understandable to the general public, particularly to those with developmental disabilities. *See* Hajer Chalghoumi et al., *Information Privacy for Technology Users With Intellectual and Developmental Disabilities: Why Does It Matter?*, ETHICS & BEHAVIOR (2017), https://doi.org/10.1080/10508422.2017.1393340.

[44] Jules Polonetsky & Stacey Gray, *The Internet of Things as a Tool for Inclusion and Equality*, 2 FED. COMM'N L. J. 104 (2017), http://www.fclj.org/wp-content/uploads/2017/10/69.2.1-Polonetsky-et-al.pdf.

not all watches have built-in accessibility features or are compatible with text-to-speech (TTS) technologies, braille reader applications, or displays. The limited availability of accessible products consequently restricts users' ability to consider the privacy of all products and to choose the IoT device or service that best suits their privacy needs or preferences. Instead, the privacy preferences of people with disabilities come second to product availability.

Choices Within IoT Devices and Services

At a more granular level, individual control occurs through the ability to choose different data collection settings within a particular IoT device or service. However, even if people with disabilities can access and use the IoT, being able to access such choice paradigms can be problematic. If a smart TV has a microphone that requires a button or remote to be manually switched off in order for the device to completely stop collecting audio data,[45] people with physical disabilities may be unable to turn that switch off. Without multiple mechanisms for exercising control, such as speech activation, people with disabilities may be forced into data collection even if they prefer otherwise, or they may require someone else to exercise choice on their behalf.

For people with developmental disabilities, digital monitoring devices—used to track the location, safety, and wellness of other people—can pose several privacy challenges. Typically, companies that produce digital monitoring devices do not consider the spectrum of developmental disabilities, choosing to market these devices to guardians or caretakers rather than to people with disabilities. Further, many of these devices do not allow the user, in this case the person with the developmental disability, to control who can access the video or audio streams of their devices (i.e., to authorize a user), nor are users notified when an authorized user may be tuned in by video or audio. This lack of notification about when someone is listening or watching and the inability to authorize a user are often marketed as positive features of the IoT product rather than features that deserve careful consideration before they are enabled. Even when a user with a developmental disability has a guardian, the user must have control over whether and when monitoring of their private, day-to-day activities takes place. A one-size-fits-all approach to individual control prevents people with disabilities from participating fully in the exercise of their privacy rights. IoT manufacturers should develop products with choice paradigms that encompass the full set of users' abilities in order to meet the principle of individual control.

2. Privacy Considerations: The Collection, Use, and Sharing of IoT Data *about* People with Disabilities

Respect for Context

Under the FIPPs, "respect for context" refers to the idea that companies should not collect, use, and disclose personal data in ways that are inconsistent with the context in which users provide the data. As discussed, IoT devices and services can collect a significant amount of information about users. However, for people with disabilities, this information collection, use, or disclosure could reveal more about the user than expected. Even if the IoT does not explicitly collect what many would consider to be traditionally "sensitive" or "personal" information, such as health conditions, otherwise non-sensitive data may lead to inferences that can make it more sensitive or revealing for people with disabilities than for those without disabilities. For example, data collection on a user's mouse movements while browsing could potentially reveal a physical disability.

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

Another example is a fitness tracker that detects step counts and records acceleration, which may reveal detailed information about a person's disability. While data collected from the step counts are not covered by sector-specific privacy regulations such as the Health Insurance Portability and Accountability Act (HIPAA), conclusions could be drawn, based on the data collected, about a user's health status or medical condition. If a fitness tracker data set reveals that a user's acceleration rate often increases while the step count remains constant, the company could infer that the user is in a wheelchair.[46] Data can reveal highly sensitive factors about users, and depending on the type of product, data uses, and controls, the same data may be subject to very different user privacy preferences.[47] Such inferences could be used to market to individuals or to sort them into particular customer segments, which, in turn, could lead to limited choices or offensive stereotyping.[48] Companies should be aware that different data types collected by the IoT about their users and the uses of such data may raise various privacy risks and potentially contradict users' expectations.

Focused Collection

Under the FIPPs guidance, consumers have a right to reasonable limits on the personal data that companies collect and retain. Limiting data collection and disposing of or de-identifying unnecessary data is a best practice and can help companies to mitigate privacy challenges. This is especially important for data collected about people with disabilities and their interaction with IoT devices and services, because the data collected about these users can identify them as having a particular disability, even when that disability might otherwise not be apparent to an observer. Further, for people with disabilities, what constitutes a "reasonable limit" of data collection may be different than what applies to people without disabilities.

Further, many people with disabilities fear that even if they have not disclosed their disability to certain sources or entities, data collection may reveal their conditions and potentially lead to discriminatory practices in employment, housing, or education, even if such practices are illegal under the Americans with Disabilities Act (ADA). For example, advertising technology companies can infer whether someone is using an assistive web extension, such as a text-to-speech or colorblind-sensitive display plugin. Browsers typically broadcast the plugins in routine web traffic. Companies could use this knowledge to infer disability and potentially profile and discriminate against users on the basis of that disability.[49]

---

[46] Numerous activity trackers now detect various wheelchair pushes, including the Apple watch, the Fitbit Flex, and Freewheel.

[47] For instance, one person may be comfortable sharing their location publicly on social media pages, whereas others may choose settings to keep that information private. *See* Rosie Spinks, *Using a Fitness App Taught me the Scary Truth about Why Privacy Settings are a Feminist Issue*, QUARTZ (Aug. 1, 2017), https://qz.com/1042852/usinga-fitness-app-taught-me-the-scary-truth-about-why-privacy-settings-are-a-feminist-issue/.

[48] *See* Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES, Feb. 16, 2012, http://www.nytimes.com/2012/02/19/magazine/shopping-habits.ht.

[49] Last year, it was reported that the Alexa button in Amazon's iPhone app had been disabled for users of Voiceover, the iPhone's built-in screen reader. The Alexa button was available only when people opened the Amazon app when Voiceover was not running; if Voiceover was running when the app was opened, the button never appeared, even if Voiceover was turned off after the Amazon app was launched. While the problem was eventually addressed, it prompted discussion regarding the challenges faced when a developer chooses to modify an interface based on whether an end-user is also a user of accessible technology. *See*: Opinion: Shady Code Alert: Amazon iPhone App Detects Voiceover and Quietly Disables Alexa, available at https://www.blindbargains.com/bargains.php?m=17549.

Another example is the Accessibility Object Model (AOM),[50] a Javascript API being developed by web browser vendors to facilitate the use of assistive technologies on the web by giving websites more context about an accessibility device or service's interactions with a website. When adopted by the World Wide Web Consortium (W3C), the AOM will create a standardized way for browsers and accessible devices to communicate, thus allowing people with disabilities to more easily browse websites by using their assistive devices or services (i.e., the devices and services are less likely to be blocked or incompatible with the websites). However, in doing so, the AOM will automatically and necessarily expose the fact that an accessibility device exists and, thus, that the user has a disability.[51] People with disabilities and companies should be aware that the use of certain services or devices and the data collected through routine practices may potentially reveal an otherwise unobservable disability.

Security

The FIPPs framework states that IoT users have a right to the secure and responsible handling of personal data. While a data disclosure involving IoT data may not pose significant issues for many users of the device, for people with disabilities this information could reveal a uniquely sensitive health condition. The consequences of IoT disclosures or security failures may pose more serious consequences for people with disabilities than for those without disabilities. When the IoT collects and retains large amounts of data about people with disabilities, this increases the potential impacts associated with a data breach, regarding both data stored locally on the IoT itself and in the cloud.

While many IoT devices and services send data to the cloud and use powerful computing to produce valuable insights and improve products or create new ones, cloud-based infrastructure has introduced potential vulnerabilities, including data breaches, denial of service attacks, and data loss. Moreover, many IoT devices and services have fewer protections from compelled disclosure and do not use secure messaging techniques, such as encryption or transmitting data over hypertext transfer protocol secure (HTTPS) connections. Such insecure transmissions can potentially produce improper data disclosures and data leakage. Companies also will need to ensure that IoT devices and services are capable of upgrading their security protocols as new threats arise and address potential vulnerabilities of those IoT devices and services that are non-upgradable to protect users' data. As the IoT collects personal and sensitive information about people with disabilities, data disclosures can produce damaging results to personal and professional relationships, especially if a disability was not known publicly. Consequently, both subjective impacts (e.g., discrimination based on a revealed condition) and objective impacts (e.g., losing a job because of a revealed condition) can result from poor security practices or failures.

Further, as technology provides more opportunity for people with disabilities to enhance their privacy, mobility, and safety, it may also introduce greater risks that users' information may be compromised by the private sector, government (particularly surveillance), or bad actors. In the United States, courts typically grant reduced protections to personal information that individuals voluntarily disclose to a third party (e.g., banks, phone companies, or internet service providers). Under this "third-party doctrine," courts usually hold that a person cannot have a reasonable expectation of privacy regarding such information, increasing the government's ability to obtain data from IoT devices and

---

[50] Alice Boxhall et al., ACCESSIBILITY OBJECT MODEL (2018), https://wicg.github.io/aom/spec/ (last visited Jan. 14, 2018).

[51] Lukasz Olejnik, *Designing Accessible Web with Privacy – When Web Browsing Reveals Information*, SECURITY, PRIVACY & TECH INQUIRIES (Oct. 29, 2018), https://blog.lukaszolejnik.com/designing-accessible-web-with-privacy-when-web-browsing-reveals-information/

services without a warrant.[52] What is considered voluntary information sharing with a third party may not be as straightforward for people with disabilities, because use of an IoT device or service and subsequent data sharing may be essential for their full participation in society. Thus, even if companies secure data, personal information may be subject to law enforcement access under this doctrine. In light of this potential privacy risk, people with disabilities and advocacy groups may want to consider promoting strong encryption in IoT devices and services as well as reforming the Electronic Communications Privacy Act (ECPA).[53] It is important that companies prevent technology from creating new vulnerabilities for the communities they serve. Serious prioritization of cybersecurity is required to ensure that these users are not at greater risk due to their use of such technology.

[52] United States v. Miller, 425 U.S. 435, 443 (1976).; Smith v. Maryland, 442 U.S. 735, 744 (1979).

[53] ECPA is a 1968 law designed to prevent unauthorized access to private electronic communications.

Table 1: The FIPPs and Privacy Considerations of People with Disabilities and the IoT

FIPP	FIPP Description	Unique Impact on People with Disabilities	Example
Privacy Considerations: The Use of the IoT *by* People with Disabilities			
Transparency	Consumers have a right to easily understandable and accessible information about privacy and security practices.	Transparency mechanisms can exclude some people with disabilities when the mechanisms are provided through only one form of communication, i.e., when consent is obtained or notice is provided about data collection.	Smart speakers that use visual signals to notify users when the device is collecting audio data without providing other cues, such as auditory or haptic notifications.
Individual Control	Companies should provide users the right to control which personal data companies collect from them and how they use it.	People with disabilities are limited in their ability to choose among different IoT devices and services and to choose different data collection settings for particular IoT devices or services.	Smart TVs with microphones that require a button or remote to be manually switched off in order for the device to cease audio data collection, without other mechanisms for exercising control, such as speech activation.
Privacy Considerations: The Collection, Use, and Sharing of IoT Data *about* People with Disabilities			
Respect for Context	Companies should not collect, use, or disclose personal data in ways that are inconsistent with the context in which users provide the data.	Information collection, use, or disclosure may be more sensitive or revealing for people with disabilities than for people without disabilities.	Fitness trackers may infer that an individual is in a wheelchair and market to that individual based on their wheelchair use or sort them into particular customer segments.
Focused Collection	Consumers have a right to reasonable limits on the personal data that companies collect and retain.	What constitutes a "reasonable limit" of data collection may be different for people with disabilities than it is for those without disabilities.	Through routine web traffic, advertising technology companies may infer the use of an assistive plugin, which can reveal an otherwise unobservable disability online.
Security	Consumers have a right to secure and responsible handling of personal data.	IoT security failures may pose more serious consequences for people with disabilities than for those without disabilities.	Cloud-based infrastructure can be vulnerable to denial of service attacks, data breaches, data loss, etc., and can lead to improper disclosure of sensitive information about people with disabilities.

B. The Privacy of Others

While there are many privacy challenges for people with disabilities when using the IoT, devices and services designed for such people may also impact those without disabilities. Many IoT devices and services designed for people with disabilities, specifically sensory disabilities, use cameras or microphones to help people navigate or access the world around them. While these products may enhance the independence, safety, and/or the ability of people with disabilities to participate fully in life, they can also infringe on the privacy of others.

For instance, recent improvements in facial recognition allow systems to recognize and learn the people with whom a person with disabilities interacts, as well as classify age, emotion, and more. For example, products such as Aira or Microsoft's Seeing AI app help people with disabilities navigate through spaces and conversations with others in their environment. However, these same devices can impact the personal privacy of those around them, especially if the devices are on or recording in private spaces or property, such as a restroom, or if someone is unaware of the use of identification systems.[54]

How IoT devices and services interact with individuals who are not users is an important consideration in these systems' development. Companies will need to implement varying levels of consent mechanisms (opt in versus opt out) depending on the specific context and consider whether the person being identified is already affirmatively connected to the facial recognition system. Likewise, even when consent and notice mechanisms may be generally sufficient, they may be challenging for those with disabilities who are less likely to be aware of signage or the presence of cameras. Companies should anticipate potential friction between more-common privacy expectations and the lesser-known uses of the IoT by people with disabilities, and establish clear norms to enable the necessary tradeoffs.

III. A Way Forward

In an era increasingly defined by rapid technological innovation, the future success of the IoT will depend in large part on ensuring that the needs and expectations of potential IoT users are adequately addressed. Through the lens of the FIPPs, we can better understand the unique privacy considerations and tensions that people with disabilities may face when using IoT devices and services. While the FIPPs apply to all users, they also can shed light on how IoT devices and services may uniquely impact people with disabilities.

When determining how to appropriately address the unique privacy considerations posed by people with disabilities' use of the IoT, companies, policymakers, and other stakeholders should consider the FIPPs and their potential role in making IoT devices and services not only accessible but also privacy protective for the disability community. Below we present actionable recommendations that will not only promote IoT access and inclusion, but also address some of the unique privacy considerations faced by people with disabilities when using IoT devices and services.

[54] Aira's live agents are instructed not to film or record if the user is in a restroom or other private spaces. The Aira app also has a privacy mode that allows the user to stop transmitting audio and video in such situations.

1. Prioritize Inclusive Design

While some technologies incorporate universal or accessible design, there are still many technologies that people with disabilities cannot access. A handful of technology companies have begun to experiment with building technologies that include accessibility as a consideration.[55] However, all too often, technology companies only consider accessibility after they have built their devices. Accessible design is often not incorporated into new technologies because of limited accessible-design experience, lack of awareness of accessible-design standards, and reluctance to invest in accessibility. Technology companies are also traditionally slow to recognize the beneficial impact of accessibility features on their customer base.[56]

For example, many social media websites or apps have created alternative text features that allow users with visual disabilities to receive a description of the contents of an image via voice-over technologies, rather than simply being told that an image is present on the screen. However, these alternative text features are not typically enabled automatically, and instead, require users to enable the feature through the settings option, i.e., users must opt in to the alternative text features. While these features can enhance people with visual disabilities' use of the IoT, the benefit of such features may be limited if they are not a default setting or opt out.[57] Companies should seek the perspectives and views of people with disabilities to understand how default settings impact the usability of the technology. Further, companies that have built accessibility features or default privacy settings into their products could provide broader education and notification to all users about these available features. In doing so, they may foster a culture of inclusion.

The right time to address accessibility is at the beginning of the technology-design process. For example, members of the disability community have advocated for deployment of autonomous vehicles (AV). As AVs are developed, they must be created with accessibility in mind. Physical accommodations (such as wheelchair lifts, ramps, and accessible door handles) and accessible navigation interfaces that use voice commands could be included to ensure that people with physical disabilities and those who are blind or have visual disabilities can access such vehicles. While many people with disabilities do not drive, this new technology could be a paradigm shift for enhancing their independence and mobility. Accessibility and the privacy of people with disabilities should not be an afterthought for the IoT and new technology developers. Accessibility should be integrated at the earliest possible iteration of IoT design and should be maintained throughout product life cycles, including updates.[58]

---

[55] For example, in 2018, Microsoft announced a new initiative called the AI for Accessibility Initiative, a $25 million five-year initiative to help the disability community get employed, form social connections, and fully participate in modern life. Mark Sullivan, *Microsoft Announces $25M Initiative to Create Apps that Help the Disabled*, FAST COMPANY, May 7, 2018, https://www.fastcompany.com/40568730/microsoft-announces-25m-initiative-to-create-apps-that-help-the-disabled.

[56] While certain standards exist regarding the accessibility of IoT devices, including ISO Guide 71,# ESTI EN 301 549, W3C's Web Content Accessibility Guidelines (WCAG) 2.0, and Section 508 of the Rehabilitation Act, none of these regulations provide principles related to privacy.

[57] Companies recently have begun to build accessible default settings. For example, Facebook has recently added a default facial recognition feature used with an automatic alternative-text tool aimed to help people with visual disabilities identify people in photos or videos. Facebook users may opt out of the feature. *See* Camila, Domonoske, *Facebook Expands Use of Facial Recognition to ID Users in Photos*, NPR, Dec. 19, 2017, https://www.npr.org/sections/thetwo-way/2017/12/19/571954455/facebook-expands-use-of-facial-recognition-to-id-users-in-photos.

[58] People with disabilities have noted that, in many instances, they have purchased products that suddenly became inaccessible to them after updates to the associated app rendered the products inoperable with Voiceover or another screen reader.

2. Promote Research and Innovation

To successfully build the IoT with universal or accessible design, qualitative and quantitative research is needed to understand how people with disabilities use the IoT and feel about its current privacy landscape. Surveys and studies exploring differences in the data-sharing preferences of people with disabilities are necessary to reveal the barriers to IoT accessibility and to ensure that the development of new IoT products incorporates disability perspectives. Specific research on particular disability communities (i.e., deaf or hard-of-hearing, blind, and other communities) and their privacy preferences would also help the IoT designers to better adapt IoT devices and services to fit the needs of all users.

Companies and players in the IoT industry also should seek to produce innovative solutions to address users' concerns regarding privacy and enhance technology adoption. Data collected from interactions between the IoT and people with disabilities can be used to support the development of new IoT technologies and enhance existing IoT devices and services. Innovation is needed to produce novel forms, functions, and modalities through which people with disabilities can interact with the technology. For example, technologies such as TippyTalk,[59] an enhanced augmentative and alternative communication (AAC) platform, allows people with developmental disabilities to communicate by translating customized pictures into personalized text messages.

Further, AI innovation may allow technology to play a greater role in helping people with disabilities navigate the space around them, participate more fully in everyday life, and live more independently in their communities. Facial, image, object, and voice recognition; natural language processing; and automation are continually implemented in assistive technologies to bridge the gaps experienced by people with disabilities. Companies developing AI technologies should be aware of the potential benefits of such technologies for people with disabilities, and they should incorporate accessible or universal design as they develop the technologies.

3. Build Privacy-by-Design Approaches

While data derived from people with disabilities' use of the IoT may provide insights into their situations and can be used to benefit individuals and society, this information can also be used in ways that raise concerns about individual privacy. To integrate privacy into IoT devices and service development, industry leaders should promote privacy-by-design approaches. Privacy-by-design can help ensure that companies consider the sensitive nature of the data being processed during the building of IoT products, which can help increase people with disabilities' use of the IoT. Companies also should consider the diversity of users' needs (e.g., auditory, visual, or haptic) and incorporate such considerations when developing privacy disclosures, notices, and other controls within IoT products. Further, the disability community's reliance on the IoT to help them participate more fully in everyday life only makes it more necessary for companies to protect their customers' privacy and enhance their trust in data collection, sharing, and use. Companies should implement technological controls that are proportionately designed to consider the sensitive nature of the data collected from the IoT used by people with disabilities.

Technologies also are increasingly created to replace or augment roles, systems, and services previously operated or performed by people, such as TTY, text-to-speech (TTS) applications, and the telecommunications device of the deaf (TTD). While human service providers must adhere to

[59] TIPPYTALK, http://www.tippy-talk.com/ (last visited Jan. 14, 2019).

confidentiality and privacy standards, such as the National Association of the Deaf (NAD) and the Registry of Interpreters for the Deaf (RID) Code of Professional Conduct[60] or the Center for Medicare & Medicaid Services (CMS) Home and Community Based Services (HCBS) Final Regulation,[61] these technologies are not required to hold the same privacy values. As the IoT augments and replaces current systems and services used by people with disabilities, existing privacy provisions should be integrated into the design of the technology and preserved.

4. Foster Cross-Sector Collaborations

Collaborations among advocates, academia, policymakers, and industry can help to integrate IoT use among people with disabilities and develop IoT solutions that meet their current and anticipated needs. For example, very few navigational aid options exist for people with visual disabilities in indoor spaces (indoor wayfinding). Beacons have been suggested as IoT devices that could be used to create digital maps that allow people with visual disabilities to navigate indoor spaces. Beacons are small, inexpensive radio transmitters that broadcast Bluetooth low energy (BLE) signals, which can be detected by mobile devices, including smartphones, to infer proximity more accurately than Wi-Fi localization can.[62] Typically, beacons are closed—a user must have an authorized app installed with permission to access the beacon. From a business point of view, private entities that use beacons want them to be closed and proprietary. However, people with disabilities could benefit greatly from access to such proprietary beacons to aid their indoor wayfinding. Cities working to deploy beacons[63] also have the opportunity to partner with developers to harness existing technology and create access to beacons through authorized apps or other technologies[64] so that people with visual disabilities can navigate indoor spaces. 5G connectivity (and beyond) and smart cities initiatives have also been viewed as unique opportunities for multi-stakeholder engagement to ensure that universal and accessible design are taken into account.

---

[60] REGISTRY OF INTERPRETERS OF THE DEAF, CODE OF PROFESSIONAL CONDUCT (2005), https://www.rid.org/ethics/code-of-professional-conduct/.

[61] Medicaid Program, Final Rule, 79 Fed. Reg. 11 (Ctrs. for Medicare & Medicaid Servs., U.S. Dep't of Health & Hum. Servs. Jan. 16, 2014), https://www.gpo.gov/fdsys/pkg/FR-2014-01-16/pdf/2014-00487.pdf.

[62] X. Zhao et al., *Does BTLE Measure up Against WiFi? A Comparison of Indoor Location Performance*, 20TH EUROPEAN WIRELESS CONFERENCE, BARCELONA, Spain (2014).

[63] Some cities have begun using beacon technologies in public spaces. For example, New York's Penn Station has partnered with Zyter and indoor.rs in 2017 to place over 400 BLE beacons in Penn Station and create an app called FindYourWay. The app provides real-time information to help users navigate the station. While the app is not designed specifically for people with disabilities, this partnership demonstrates the real potential for accessible technologies to be created through multi-stakeholder engagement and to harness the power of existing beacons for people with visual disabilities. See *Patrick McGeehan, Lost in Penn Station? Amtrak Has an App to Guide You*, N.Y. TIMES (2017), https://www.nytimes.com/2017/12/13/nyregion/penn-station-amtrak-findyourway-app.html.

[64] Groups such as Wayfindr, a nonprofit organization committed to creating a benchmark in standards for digital wayfinding on mobile devices, has created an Open Standard that provides tools including an open-source demo app to implement consistent, audio wayfinding solutions for BLE beacons, which has been approved by the International Telecommunications Union. INTERN'L TELECOMM. UNION, AUDIO-BASED NETWORK NAVIGATION SYSTEM FOR PERSONS WITH VISION IMPAIRMENT (2017), https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=13185&lang=en. Wayfindr has also recently partnered with the London Underground to create digital navigation systems for people with visual disabilities; trials are currently ongoing throughout London and in other cities around the world. See Rob Price, *A Google-Backed Project to Help Blind People Navigate with Smartphone Got a Boost from the UN*, BUSINESS INSIDER (Sep. 30 2017), http://www.businessinsider.com/wayfindr-google-backed-blind-navigation-approved-un-trials-2017-9.

5. Enhance Awareness of Data Risks and Benefits

IoT developers, policymakers, and other stakeholders should consider the risks and benefits of IoT and data-reliant technologies for people with disabilities. This should include not only the potential enhanced risks that people with disabilities may face when using the IoT, but also the particularly high value that some of these same technologies and increased data collection could provide to those communities.

It is a best practice for companies not to collect more data than they need (focused collection), to mitigate potential privacy risks. At the same time, high-quality data are needed to improve companies' understanding of the needs of people with disabilities, mitigate the data divide, and enable developers to build better products and services for such people. We need to develop practices to balance these considerations, for example, by allowing people to opt in to increased data collection when the data are used for specified beneficial purposes.

Further, in some cases, increased data collection from the disability community may actually lead to increased privacy protections for this community. For example, consider Aira, a pair of smart glasses that connect to a human agent to help users with visual disabilities navigate and understand visual details of the space around them. Aira Tech Corporation is working to integrate AI into the product to take over some of the tasks of the human agent, such as navigation.[65] While adding AI into Aira will require increased data collection and use, the decreased need for human agents to guide users will certainly enhance users' privacy. Stakeholders should weigh the benefits of enhancing user privacy against the potential privacy risks of increased data collection when seeking to produce new IoT devices or services or implement new features.

People with disabilities should take a proactive role in their privacy and voice their views on the privacy challenges they face when using IoT devices and services. This could include engaging in debates on ECPA reform, encryption of sensitive data, and potential national privacy legislation.[66] As new technologies such as facial recognition and AVs are developed, the disability community should participate in policy discussions about the accessibility and privacy designs of such products. Given the increase in regulations and codes that can restrict data collection, use, and sharing, people with disabilities and advocates should consider speaking out about how such restrictions may impact their communities. By providing opportunities to learn more about the disability community's unique needs and contributing to the development of better IoT products and services, data collection may provide great benefits to the disability community. People with disabilities and advocates should encourage policymakers to consider their unique circumstances regarding data collection and privacy.

---

[65] Chris Kornelis, *AI Tools Help the Blind Tackle Everyday Tasks*, WALL STREET J. (May 28, 2018), https://www.wsj.com/articles/ai-tools-help-the-blind-tackle-everyday-tasks-1527559620.

[66] There also may be opportunities to advocate that laws be interpreted to enhance access to IoT devices and services to fulfill mandates. For example, Sec.36.303 of the Americans with Disability Act (ADA) requires public accommodations to "take those steps that may be necessary to ensure that no individual with a disability is excluded, denied services, segregated or otherwise treated differently than other individuals because of the absence of auxiliary aids and services." It could be argued that in order for one to achieve those access and inclusion rights as afforded in Section.36.303, one has the right to use technology, particularly as technologies are increasingly becoming integral to our society. With the increased use of technologies, there will inevitably be an increase in data collected about the disability community, which, in turn, can potentially provide great benefit to the community and IoT developers. 28 CFR 36.303.

CONCLUSION

While IoT devices and services provide many benefits to people with disabilities, society, and industry, the IoT raises particular privacy challenges for people with disabilities. When people with disabilities use the IoT, companies should consider not only the privacy considerations unique to this group, but also the privacy of third parties that may come into contact with the IoT. The FIPPs (transparency, individual control, respect for context, focused collection, and security) provide a framework for recognizing and understanding the unique privacy considerations faced by the disability community when using IoT devices and services:

- When provided through only one form of communication, transparency mechanisms can exclude some people with disabilities;
- People with disabilities are limited in their ability to choose among IoT devices and services and within data-collection settings for particular IoT devices or services;
- Information collection, use, or disclosure may be more sensitive or revealing for people with disabilities than for those without disabilities;
- What constitutes a "reasonable limit" of data collection may be different for people with disabilities than it is for those without disabilities; and
- The consequences of IoT security failures may pose more serious consequences for people with disabilities than for those without disabilities.

With the FIPPs as a guide and a firm understanding of the unique privacy considerations of people with disabilities, developers can protect their privacy.

To address these privacy considerations, companies, IoT architects, developers, product owners, and other stakeholders should: (1) integrate accessibility into the earliest possible iteration of IoT development; (2) seek ways to collect data specifically to inform the development of new IoT technologies and enhance existing IoT devices and services, without overriding people's privacy preferences; (3) implement technological controls that are proportionately designed to consider the sensitive nature of the data collected from the IoT used by people with disabilities; (4) facilitate collaborations among advocates, academia, policymakers, and industry to help integrate IoT use among people with disabilities and develop IoT solutions that meet their current and anticipated needs; and (5) acknowledge both the benefits and risks of data collection from people with disabilities. A combination of industry changes, research, and collaborations is necessary to address the privacy considerations of people with disabilities when using the IoT. We can begin by recognizing and incorporating the unique privacy considerations of people with disabilities in the future of the IoT.

APPENDICES

APPENDIX I. STAKEHOLDERS

Special thanks to the organizations listed below, whose members provided invaluable feedback during the drafting of this paper. This paper does not necessarily reflect their views.

Access Now
Aira
American Association of People with Disabilities
American Civil Liberties Union
American Council of the Blind
AT&T
Autistic Self Advocacy Network
Call for Action
Cellular Telecommunications Industry Association
Center for Democracy and Technology
Coleman Institute for Cognitive Disabilities
Comcast
Comcast Innovation Fund
Consortium for Citizens with Disabilities
Facebook
LGBT Technology Partnership & Institute
Microsoft
National Network to End Domestic Violence
Puffin Innovations
Sprint
Toyota
United Spinal Association
Verizon
Wavio

APPENDIX II. TAXONOMY OF THE IOT USED BY PEOPLE WITH DISABILITIES

The Internet of Things is a topic of increasing technical, social, and economic significance. However, no clear and universally accepted definition exists for the IoT. The term is broad-sweeping and not easily defined. As one author describes it, the IoT "seems to mean everything and nothing."[67] The IoT covers various cyber-physical systems, ranging from drones to wearables, and the industry is changing at such a fast pace that the associated policy, legal, and regulatory structures can barely keep up.

The IoT taxonomies currently available provide a shared lexicon that helps participants in the IoT ecosystem, i.e., consumers, academics, developers, and more, communicate across organizational boundaries, which, in turn, helps stakeholders better understand and address emerging IoT issues. The IoT taxonomies also help to identify gaps in IoT projects (e.g., product development), often spurring innovation. However, taxonomies for the IoT typically have not focused on the relationship between IoT products and the disability community. While the IoT provides convenience to all consumers, it can be life-changing for people with disabilities.

In this section, we provide an overview of the IoT devices and services used by people with disabilities. We hope that this taxonomy will advance the conversation on inclusive IoT and, in particular, illuminate privacy concerns that are central to people with disabilities and opportunities for future product development and policy work. In this appendix, we describe three categories of the IoT used by people with disabilities: (A) the IoT accessible to people with disabilities, (B) the IoT repurposed by people with disabilities, and (C) the IoT designed for people with disabilities.[68]

A. The IoT Accessible to People with Disabilities (Universal Design)

The IoT accessible to people with disabilities are either IoT products designed to incorporate the needs of people with disabilities or IoT products that are accessible and useful to people with disabilities even though accessibility was not at the forefront of product design.[69] The smart speaker, for example, was developed for the broader consumer market but is accessible to people with disabilities because of the nature of the product itself.[70] The same features that promise comfort and convenience to general users (e.g., being able to control lights, temperature, and locks) can provide independence and more for the hundreds of thousands of smart-speaker owners who have

---

[67] Pavel Smutny, *Different Perspectives on Classification of the Internet of Things*, 2016 17TH INTERNATIONAL CARPATHIAN CONTROL CONFERENCE (2016), http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7501184&isnumber=7501055.

[68] See Appendix, Figure 1 for examples of the three categories of IoT used by people with disabilities.

[69] Allen St. John, *Amazon Echo Voice Commands Offer Benefits to Persons with Disabilities*, CONSUMER REPORTS (Jan. 20, 2017), https://www.consumerreports.org/amazon/amazon-echo-voice-commands-offer-big-benefits-to-users-with-disabilities/ (last visited Jan. 14, 2019). "Amazon has several assistive-technology teams that help to develop products for this market as well adding features to current products like the VoiceView screen reader for Amazon's tablet and Fire TV platforms. However, those teams didn't need to add anything to the voice-command smart speakers, so growth of this informal "adaptive Alexa" movement has largely been organic, spread largely by word of mouth." *Id.*

[70] Sixteen percent of Americans (39 million people) own a smart speaker, and most (64%) of those owners said they purchased the speakers because they planned to use them to control smart home devices. Sarah Perez, *39 Million Americans now Own a Smart Speaker*, TECH CRUNCH (Jan. 12, 2018), https://beta.techcrunch.com/2018/01/12/39-million-americans-now-own-a-smart-speaker-report-claims/ (last visited Jan. 14, 2019).

disabilities. Some argue that if companies followed universal design principles, their technology would be accessible to all, reducing the need for "special" technology solutions that often make up a small portion of the market. However, given the diversity of needs across the disability communities, it appears that there will always be a need for specific design solutions. The IoT accessible to people with disabilities will likely not be accessible to *all* people with disabilities.

B. The IoT Designed for People with Disabilities (Accessible Design)

The IoT designed for people with disabilities fall under the category of accessible design: these products are intended for use entirely or primarily by people with disabilities. Many of the products in this category were created by people with disabilities for people with disabilities, to address an unmet need.[71] For example, Wavio—a sound-capturing unit that can be programmed to hear various sounds, ranging from the sound of a doorbell to a crying baby—was created when its founder, who is deaf, moved out on his own and realized that such a device was needed to help deaf communities maintain their independence.[72] Other examples of the IoT designed specifically for people with disabilities include smart canes, which track the user's location and tells someone if they have fallen, left a certain area, or need help; smart shirts, which take the music being performed during a concert and translate it into the haptic sensations; and apps such as TapTapSee, which helps users with visual disabilities to recognize objects by taking a photo and identifying it through a database of crowdsourced images. While there are many great IoT projects for people with disabilities, there is more work to be done. Unfortunately, many of the projects that could make an enormous difference in the lives of people with disabilities are not yet in production because of a lack of funding.

C. The IoT Repurposed by People with Disabilities

The IoT repurposed by people with disabilities refers to a category designed for and marketed to a broader consumer audience but that has various unconventional or unexpected assistive uses. Consider smart speakers as an example: while all users, including those who have disabilities, may use the voice-activated command feature to control lights, locks, temperatures, etc., people with disabilities use smart speakers in a way that others do not. For example, deaf people may use the voice-to-text features on smart speakers to communicate with non-deaf people around them.

[71] Some products in this category exist because of the ADA mandate that public facilities and services be accessible to people with disabilities.

[72] *Wavio*, DEAF PEOPLE AND TECHNOLOGY COMPENDIUM, https://deaftechcompendium.wordpress.com/2017/05/09/wavio/ (last visited Jan. 14, 2019).

APPENDIX III: EXAMPLES OF THE IOT COMMONLY USED BY PEOPLE WITH DISABILITIES

Accessible to People with Disabilities	Repurposed by People with Disabilities	Designed for People with Disabilities
• **Alexa and Google Home:** smart home assistants[i] • **Amazon Dash**: restocks household items[ii] • **Driver-Assistance Technology**: semi-autonomous vehicle operation[iii] • **Fitbit and Apple Health**: health and fitness trackers[iv] • **Indoor Location Mapping**: locate accessible services in public places (e.g., ramps and elevators)[v] • **Lechal Shoes**: wearable navigation assistant[vi] • **Livescribe Smart Pens**: records written notes and accompanying audio • **Athos**: clothing that tracks heart rate and breathing data[vii] • **Ring Alarms**: motion-sensor-equipped security system[viii] • **Tile**: Bluetooth tracking device[ix] • **Pillo**: digital health assistant/pill dispenser/reminder system[x]	• **Find My Friends App:** used for security purposes[xi] • **Glide App**: live video messenger app that can be helpful for individuals to sign messages to each other[xii] • **Nest**: home automation and security system used to track whether certain areas of the house were accessed[xiii] • **PracticeSuite**: used to schedule medical appointments; helpful for individuals who do not use the phone to call[xiv] • **Philips HUE Light Bulbs**: "if this, then" color changing bulbs, e.g., flash green for doorbell, red for fire[xv] • **Text-To-Voice Messaging:** used to converse with people around the user[xvi]	• **ADAMM Intelligent Asthma Monitoring:** predicts asthma attacks[xvii] • **AdhereTech:** smart pill bottles ensure medication adherence[xviii] • **Dot:** smart braille watch[xix] • **Dring Connected Cane:** smart cane with GPS tracking and fall detection[xx] • **Lively:** monitors older adults' safety and habits[xxi] • **Oticon Opn:** hearing aid that can communicate with other connected devices[xxii] • **OrCam:** artificial vision technology for people who have visual disabilities[xxiii] • **Sound Shirt:** a wearable device that converts sounds into nuanced vibrations in real time, so that people who are deaf can experience concerts[xxiv] • **Voiceitt:** speech recognition technology designed to understand non-standard speech[xxv] • **TapTapSee App:** assists users with visual disabilities in recognizing objects[xxvi] • **TippyTalk:** an enhanced augmentative and alternative communication (AAC) platform that translates customized pictures into personalized text messages[xxvii] • **Toyota Project BLAID:** navigation for people who have visual disabilities[xxviii]

Appendix III Endnotes

[i] *All things Alexa*, AMAZON, https://www.amazon.com/Amazon-Echo-And-Alexa-Devices/b?ie=UTF8&node=9818047011 (last visited Jan. 14, 2019); GOOGLE HOME, https://store.google.com/au/product/google_home (last visited Jan. 14, 2019),

[ii] *Amazon Dash*, AMAZON, https://www.amazon.com/b?ie=UTF8&node=17729534011 (last visited Jan. 14, 2019).

[iii] Automakers are constantly developing driver-assistance technologies such as adaptive cruise control, automatic breaking, blind spot detection, and GPS navigation. *See Driver Assistance Technologies*, U.S. DEP'T OF TRANSPORTATION, https://www.nhtsa.gov/equipment/driver-assistance-technologies (last visited Jan. 14, 2019).

[iv] FITBIT, https://www.fitbit.com/home (last visited Jan. 14, 2019); *Apple Watch*, APPLE, https://www.apple.com/watch/ (last visited Jan. 14, 2019)

[v] AXSmap, https://www.axsmap.com/ (last visited Jan. 14, 2019).

[vi] LECHAL, http://www.lechal.com/initiative.html (last visited Jan. 14, 2019).

[vii] ATHOS, https://www.liveathos.com/shop (last visited Jan. 14, 2019).

[viii] RING, https://ring.com/ (last visited Jan. 14, 2019).

[ix] TILE, https://www.thetileapp.com/en-us/products/mate (last visited Jan. 14, 2019).

[x] PILLO, https://www.pillohealth.com (last visited Jan. 14, 2019).

[xi] *Find My Friends: App Store Preview*, APPLE, https://itunes.apple.com/us/app/find-my-friends/id466122094?mt=8 (last visited Jan. 14, 2019).

[xii] GLIDE, https://www.glide.me (last visited Jan. 14, 2019).

[xiii] NEST, https://nest.com/ (last visited Jan. 14, 2019).

[xiv] PRACTICESUITE, https://www.practicesuite.com (last visited Jan. 14, 2019).

[xv] *5 Promising Examples of IoT and Wearable Devices that Enable People with Disabilities*, MEDIUM (last visited Jan. 14, 2019), https://medium.com/@imn/5-promising-examples-of-iot-and-wearable-devices-that-enable-people-with-disabilities-f50df601e046.

[xvi] *See, e.g.*, ROGERVOICE, https://rogervoice.com/en/ (last visited Jan. 14, 2019); TOUCH VOICE, https://touch-voice.com/uc/content/about-touch-voice-gold-web-app (last visited Jan. 14, 2019).

[xvii] HEALTH CARE ORIGINALS, http://healthcareoriginals.com/ (last visited Jan. 14, 2019).

[xviii] ADHERETECH, https://www.adheretech.com/ (last visited Jan. 14, 2019).

[xix] DOT, https://dotincorp.com/ (last visited Jan. 14, 2019).

[xx] DRING, https://dring.io/ (last visited Jan. 14, 2019).

[xxi] GREATCALL, https://www.greatcall.com/devices/lively-wearable-senior-activity-tracker/ (last visited Jan. 14, 2019).

[xxii] OTICON, https://www.oticon.com/solutions (last visited Jan. 14, 2019).

[xxiii] ORCAM, https://www.orcam.com/en/ (last visited Jan. 14, 2019).

[xxiv] *The Sound Shirt*, CUTECIRCUIT, http://cutecircuit.com/soundshirt/ (last visited Jan. 14, 2019).

[xxv] VOICEITT, http://www.voiceitt.com/ (last visited Jan. 14, 2019).

[xxvi] TAPTAPSEE, https://taptapseeapp.com/ (last visited Jan. 14, 2019).

[xxvii] TIPPYTALK, http://www.tippy-talk.com/ (last visited Jan. 14, 2019).

[xxviii] News Release, Wearable Mobility Device for the Blind and Visually Impaired Being Developed by Toyota, Toyota, https://pressroom.toyota.com/releases/wearable+mobility+visually+impaired+toyota.htm (March 7, 2016).

FUTURE OF PRIVACY FORUM

1400 Eye Street, NW, Suite 450
Washington, DC 20005
fpf.org