August 20, 2018

Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20530

Re: The Intersection between Privacy, Big Data, and Competition

The Future of Privacy Forum (FPF) is a nonprofit organization that seeks to advance responsible data practices in support of emerging technologies and is supported by leaders in business, academia, and consumer advocacy.[1] We thank the FTC for this opportunity to comment on the intersection between privacy, big data, and competition.

FPF conducts empirical research,[2] publishes analyses of complex issues,[3] crafts and implements self-regulatory frameworks,[4] educates stakeholders through infographics and workshops,[5] testifies before

---

[1] The views herein do not necessarily reflect those of the Advisory Board or supporters of the Future of Privacy Forum.

[2] Future of Privacy Forum, *Beyond One Classroom: Parental Support for Technology and Data Use in Schools* (2016), https://fpf.org/wp-content/uploads/2016/12/Beyond-One-Classroom.pdf; Future of Privacy Forum, *Consumer Views Regarding Ad Blocking Technology* (2016), https://www.ftc.gov/system/files/documents/public_comments/2016/10/00065-129184.pdf; Future of Privacy Forum, *FPF Mobile Apps Study* (2016), https://fpf.org/wp-content/uploads/2016/08/2016-FPF-Mobile-Apps-Study_final.pdf.

[3] THE CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY (Evan Selinger, Jules Polonetsky, & Omer Tene, eds., Cambridge Univ. Press, 2018); Future of Privacy Forum & Immuta, *Beyond Explainability: A Practical Guide to Managing Risk in Machine Learning Models* (2018), https://fpf.org/wp-content/uploads/2018/06/Beyond-Explainability.pdf; Future of Privacy Forum, *City of Seattle Open Data Risk Assessment* (2018), https://fpf.org/wp-content/uploads/2018/01/FPF-Open-Data-Risk-Assessment-for-City-of-Seattle.pdf; Future of Privacy Forum, *Communicating about Data Privacy and Security* (2018), https://docs.wixstatic.com/ugd/e35e20_411ab2738ba54873b2995c7389ee489b.pdf; Future of Privacy Forum & Nymity, *Processing Personal Data on the Basis of Legitimate Interests under the GDPR* (2018); Future of Privacy Forum & Family Online Safety Institute, *Kids & The Connected Home: Privacy in the Age of Connected Dolls, Talking Dinosaurs, and Battling Robots* (2016), https://fpf.org/wp-content/uploads/2016/11/Kids-The-Connected-Home-Privacy-in-the-Age-of-Connected-Dolls-Talking-Dinosaurs-and-Battling-Robots.pdf; Omer Tene & Jules Polonetsky, *Beyond IRBs: Ethical Guidelines for Data Research*, 72 WASH. & LEE L. REV. ONLINE 458 (2016), https://scholarlycommons.law.wlu.edu/wlulr-online/vol72/iss3/7.

[4] Future of Privacy Forum, *Mobile Location Analytics Code of Conduct*, https://fpf.org/wp-content/uploads/2018/05/MLA-Code-v2-1-10-18.pdf; Future of Privacy Forum, *Student Privacy Pledge*, https://studentprivacypledge.org (last accessed Aug. 15, 2018).

[5] Future of Privacy Forum, *Privacy Best Practices for Consumer Genetic Testing Services* (2018), https://fpf.org/wp-content/uploads/2018/07/FPF-Genetics-Infographic-FINAL.jpg; Future of Privacy Forum, *Data and the Connected Car – Version 1.0*, (2017), https://fpf.org/wp-content/uploads/2017/06/2017_0627-FPF-Connected-Car-Infographic-Version-1.0.pdf; Future of Privacy Forum, *Financial Data Localization: Conflicts and Consequences* (2017), https://fpf.org/wp-content/uploads/2017/12/FPF_Bank-Regs_illo_01.pdf; Future of Privacy Forum, *Microphones & the Internet of Things: Understanding Uses of Audio Sensors in Connected Devices* (2017), https://fpf.org/wp-content/uploads/2017/08/Microphones-Infographic-Final.pdf; Future of Privacy Forum, *Shedding Light on Smart City Privacy* (2017), https://fpf.org/2017/03/31/shedding-light-smart-city-privacy/; Future of Privacy Forum, *A Visual Guide to Practical Data De-Identification* (2016), https://fpf.org/wp-content/uploads/2017/06/FPF_Visual-Guide-to-Practical-Data-DeID.pdf; Future of Privacy Forum & Software and Information Industry Association, Student Privacy Bootcamp, Chicago (June 26, 2018); Future of Privacy Forum & Software and Information Industry Association, Student Privacy Bootcamp, Austin (March 5, 2018); Future of Privacy Forum & Software and Information Industry Association, Student Privacy Bootcamp, Washington, D.C. (Dec. 8, 2017); Future of Privacy Forum & Information Accountability Foundation, Sustainable Innovation with Effective Data Protection in the Pacific Rim, International Conference of Data

lawmakers and agencies,[6] and examines emerging issues that can impact privacy and data practices. We urge the Commission to consider how these types of efforts – research, analysis, self-regulation, and education – can support the FTC's mission. The Commission can play an important role in supporting stakeholder work by promoting leading research, supporting credible self-regulatory frameworks, educating consumers and businesses, and highlighting emerging issues that will impact consumers and companies as they seek to enjoy the benefits of data while protecting privacy.

Below, we describe the benefits of increased FTC support for self-regulatory efforts. We also discuss an emerging issue – the intersection of consumer safeguards and technologies that empower disability communities – that has increasingly important implications for privacy, accessibility, consumers generally, and traditionally underserved users in particular.

Supporting Self-Regulation

With regard to self-regulation, we note the wide range of efforts setting out standards that have emerged from diverse organizations over the past decade.[7] As FPF begins its 10th year of activity, we look back at 10 years as authors, conveners, or participants of dozens of self-regulatory efforts over the period.[8]

The FTC has supported transparent, enforceable self-regulation as "an important tool for consumer protection," lauding self-regulatory frameworks that address issues from cross border data transfers to alcohol marketing to privacy.[9] The Commission has taken steps to ensure that companies are truthful when they make representations about their participation in self-regulatory frameworks.[10]

Protection Commissioners in Hong Kong (Sept. 25, 2017), https://fpf.org/2017/09/20/artificial-intelligence-machine-learning-and-ethical-applications/; Future of Privacy Forum et al., Refining Privacy to Improve Health Outcomes (October 26-27, 2017), http://www.triangleprivacyhub.org/2017-symposium/.

[6] *Curating a Healthier & Safer Approach: Issues of Mental Health and Counseling for our Young: Fed. Comm'n on Student Safety Meeting* (2018) (statement of John Verdi, Vice President of Policy, Future of Privacy Forum), https://fpf.org/wp-content/uploads/2018/07/Statement-of-John-Verdi-School-Safety.pdf; *Protecting Privacy, Promoting Data Security: Exploring How Schools and States Keep Data Safe: Hearing Before the H. Comm. on Educ. and the Workforce*, 115th Cong. (2018) (statement of Amelia Vance, Director of Education Privacy, Future of Privacy Forum), https://edworkforce.house.gov/uploadedfiles/testimony_vance_5.17.18.pdf; *Privacy Implications of Collecting FHV Drop-off Location Data in Proposed Rule 2016 RG 097: Hearing Before the NYC Taxi and Limousine Comm'n* (2017) (statement of Lauren Smith, Policy Counsel, Future of Privacy Forum), https://fpf.org/wp-content/uploads/2017/01/2016_0104-FPF-Oral-Comments-TLC_3.pdf.

[7] *E.g.*, Digital Advertising Alliance, Self-Regulatory Principles, https://digitaladvertisingalliance.org/principles (last visited Aug. 20, 2018); Network Advertising Initiative, *2018 NAI Code of Conduct*, https://www.networkadvertising.org/sites/default/files/nai_code2018.pdf (last visited Aug. 20, 2018).

[8] *E.g.*, Future of Privacy Forum, *Mobile Location Analytics Code of Conduct*, https://fpf.org/wp-content/uploads/2018/05/MLA-Code-v2-1-10-18.pdf; Future of Privacy Forum, *Student Privacy Pledge*, https://studentprivacypledge.org (last accessed Aug. 15, 2018).

[9] Edith Ramirez, Commissioner, Fed. Trade Comm'n, *Opening Remarks of The Federal Trade Commission Workshop on Intellectual Property Rights in Standard Setting*, 2 (June 21, 2011), https://www.ftc.gov/sites/default/files/documents/public_statements/opening-remarks-commissioner-edith-ramirez/121129codesconductremarks.pdf.

[10]*E.g.*, *In the Matter of Sentinel Labs*, Inc., FTC No. C-4608, https://www.ftc.gov/system/files/documents/cases/162_3250_c4608_sentinel_labs_decision_and_order.pdf; *In the Matter of SpyChatter, Inc.*, FTC No. C-4614, https://www.ftc.gov/system/files/documents/cases/162_3251_c4614_spychatter_decision_and_order.pdf; *In the Matter of Vir2us*, Inc., FTC No. C-4609, https://www.ftc.gov/system/files/documents/cases/162_3248_c4609_vir2us_decision_and_order.pdf.

Yet, with limited exceptions, the FTC has been active in relatively few of these efforts; the Commission rarely comments to support, oppose, or indicate its views to the public regarding the merits of particular codes of conduct, best practices, or other self-regulatory frameworks.[11] We deeply appreciate that FTC staff will meet and provide input and responses informally during the development of such efforts, when requested. But we think the agency misses a major opportunity to influence privacy practices by the conservative role it has played in this area. For example, during the NTIA privacy multi-stakeholder efforts of the previous Administration, the FTC played a fairly limited role, even when stakeholders where eager for the agency's direction and support.[12]

The Commission has an opportunity to assert a more public role and voice in self-regulatory efforts, when sought by stakeholders. Such a role would afford the FTC a significant opportunity to move industry data practices in a positive direction, by identifying self-regulatory codes or efforts that the Commission views as consistent with privacy principles articulated in law, regulation, settlement decrees, Commissioners' statements, or staff reports. Explicit public statements by the FTC regarding the value of particular self-regulatory frameworks can provide invaluable guidance to companies as they weigh whether to adopt codes of conduct or participate in such frameworks.

We do not make this suggestion as an alternative to legislative efforts for a comprehensive federal privacy law, but rather as a necessary supplement to statute. FPF has long supported a baseline, comprehensive, common sense federal law that provides consumers with meaningful protections and businesses with greater clarity about their obligations. But legislation is likely to take a generally higher level form, leaving substantial room for important best practices to be set by self-regulatory efforts. And in the absence of legislation, these efforts are even more essential.

Highlighting Emerging Issues

Attached, FPF submits a summary and key recommendations from our forthcoming report jointly authored with Henry Claypool (FPF Senior Fellow and formerly Executive Vice President of the American Association of People with Disabilities): *The Internet of Things and Persons with Disabilities: Exploring the Unique Benefits, Challenges, and Privacy Tensions*.

The paper highlights the unique benefits and privacy concerns of persons with disabilities in regards to their use of the Internet of Things (IoT). The Internet of Things has been a focus of FPF's work since our founding in 2008. FPF recognizes the enormous potential benefits of the IoT to consumers

---

[11] *See, e.g.*, 16 C.F.R. § 312.11; Leslie Fair, FTC Cases Affirm Commitment to Privacy Shield, FED. TRADE COMM'N BLOG (Sept. 9, 2017, 11:15 AM), https://www.ftc.gov/news-events/blogs/business-blog/2017/09/ftc-cases-affirm-commitment-privacy-shield; Fed. Trade Comm'n, *FTC Staff Report: Cross-Device Tracking* (2017), https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf; *Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change* 40 (2010), http://www.ftc.gov/os/2010/12/101201privacyreport.pdf; Fed. Trade Comm'n, *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising* (2009), http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

[12] Fed. Trade Comm'n, Bureau of Consumer Protection and Office of Policy Planning, *Comments to the NTIA on the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things* (June 2, 2016)*,* https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-office-policy-planning-national-telecommunications/160603ntiacomment.pdf.

and to society,[13] and acknowledges the privacy and security challenges presented by the IoT as technology evolves. FPF has worked, from the beginning, to ensure that privacy and security are integrated into the design and implementations of the IoT that involve the collection and sharing of personal information. Starting with a white paper on Privacy by Design in the smart grid (jointly authored with Information and Privacy Commissioner of Ontario, Ann Cavoukian, Ph.D.)[14] and continuing with our current work on "home devices," [15] "wearables," [16] "connected cars," [17] "drones," [18] and "smart stores," [19] FPF has acquired valuable experience and insights into the technologies and services associated with connected device ecosystems.

FPF's past work on the Internet of Things has served as a launching pad for a number of our recent initiatives, which closely examine how emerging technologies – including the IoT – impact vulnerable populations, especially persons with disabilities.[20] In a summary of our forthcoming report (below), *The Internet of Things and Persons with Disabilities: Exploring the Unique Benefits, Challenges, and Privacy Tensions*,[21] we highlight benefits of emerging technologies for persons with disabilities, and explore the unique privacy considerations that may impact persons with disabilities when using IoT devices and services. Our analysis specifically highlights how IoT devices and services may impact persons with disabilities in unique ways that may require distinct analyses under several of the Fair Information Practice Principles, specifically: transparency, individual control, respect for context, focused collection, and security. We also consider how the collection, use and sharing of IoT-derived data may be uniquely sensitive for persons with disabilities, as well as how IoT devices and services that benefit persons with disabilities may impact the privacy of others.

---

[13] The array of consumer benefits coming from the Internet of Things was underscored by the focus on connected devices at the 2014 Consumer Electronics Show. See, e.g., Kim Peterson, "Internet of Things" All the Rage at Consumer Electronics Show, CBSNews.com (Jan. 7, 2014 8:49 a.m.), http://www.cbsnews.com/news/internet-ofthings-all-the-rage-at-consumer-electronics-show/.

[14] Future of Privacy Forum & Information and Privacy Commissioner, Ontario, Canada, *Smart Privacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation* (2009), http://www.ipc.on.ca/images/resources/pbd-smartpriv-smartgrid.pdf.

[15] 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.

[16] Future of Privacy Forum, *A Practical Paradigm for Wearables* (2015), https://fpf.org/wp- content/uploads/FPF-principles-for-wearables-Jan-2015.pdf.

[17] *The Connected Car and Privacy, Navigating New Data Issues* (2014), https://fpf.org/wp-content/uploads/FPF_Data-Collection-and-the-ConnectedCar_November2014.pdf.

[18] FPF is a member of a diverse subgroup of stakeholders, including leading privacy advocates, drone organizations and companies, and associations, which have proposed drone privacy best practices. *See Multi-Stakeholder Group Finalizes Agreement on Best Practices for Drone Use*, Future of Privacy Forum, https://fpf.org/2016/04/22/progresson-drone-privacy-best-practices.

[19] FPF is providing leadership on the use of mobile location analytics in the retail environment and the associated privacy issues. *See Smart Stores*, Future of Privacy Forum, http://www.futureofprivacy.org/issues/smart-stores/.

[20] Future of Privacy Forum, *Unfairness by Algorithm: Distilling the Harms of Automated Decision-Making* (2017), https://fpf.org/wp-content/uploads/2017/12/FPF-Automated-Decision-Making-Harms-and-Mitigation-Charts.pdf; Jules Polonetsky & Stacey Gray, *The Internet of Things as a Tool for Inclusion and Equality*, FED. COMM. L. J., 69, http://www.fclj.org/wp-content/uploads/2017/10/69.2.1-Polonetsky-et-al.pdf.

[21] This paper was drafted with support from the Comcast Innovation Fund and in consultation with the American Association of Persons with Disabilities (AAPD) Technology Forum and a number of stakeholders.

We conclude by providing the following actionable recommendations that address the unique privacy considerations faced by persons with disabilities when using IoT devices and services:

1. Include Persons with Disabilities in the Design of IoT Technologies
2. Promote Research
3. Build Privacy by Design Approaches
4. Foster Cross-Sector Collaborations
5. Enhance Awareness of IoT Risks and Benefits

As the types and numbers of IoT devices and services available for and used by persons with disabilities increase, more nuanced conversations must be had about the unique privacy implications of such uses. The Commission is well positioned to lead these discussions, and to encourage stakeholders to address these privacy considerations that are unique to persons with disabilities. FPF thanks the Commission for this opportunity to submit comments and we look forward to future engagement on these topics.

Sincerely,

Jules Polonetsky, *CEO*
John Verdi, *VP of Policy*
Lauren Smith, *Policy Counsel*
Chanda Marlowe, *Christopher Wolf Fellow*
Carson Martinez, *Health Policy Fellow*

Future of Privacy Forum
www.fpf.org

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

Today, an estimated 8.4 billion connected devices are in use worldwide.[22] While there are no statistics on how many persons with disabilities use IoT devices and services, it is likely that the number is rapidly increasing due to the increase in uptake and everyday use of the IoT.[23] The IoT and its associated data is producing accessibility-related advances, ranging from smart home devices to self-driving cars. IoT devices and services are also empowering persons with disabilities to participate more fully and autonomously in everyday life by reducing some needs for human intermediaries or accommodations. Data derived from persons with disabilities' use of IoT devices and services can provide insights into the challenges and opportunities experienced by persons with disabilities, which can enhance existing IoT products or lead to development of new ones. The potential benefits of IoT devices and services for persons with disabilities are far-reaching; here are a few specific examples:

For persons with disabilities, the IoT can be transformational because it can enhance safety, mobility, independence, and privacy.
- For people who are visually impaired, the OrCam, a wearable video camera that is designed for the visually impaired, translates text to audio in real time.[24]
- For people with mobility-related disabilities: smart home technology allows users to control things in their homes that may be physically difficult to reach, such as lights, door locks or security systems.[25]
- For persons with auditory disabilities who require the assistance of TTY intermediaries to communicate, IoT devices and services such as Uni,[26] a real-time translation technology that converts sign language to grammatically correct spoken language, are allowing persons with auditory impairments to communicate without the need for a third-party translator.

For society, universal design – "the practice of designing products, buildings and public spaces and programs to be usable by the greatest number of people," and accessible design – "a design process in which the needs of people with disabilities are specifically considered," have helped create a more accessible society.[27] 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.

---

[22] Press Release: Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016, Gartner (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

[23] 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 and Dot (shown in a kitchen) have large appeal for users with disabilities

Amazon Echo Voice Commands Offer Big Benefits to Users with Disabilities, Consumer Reports (January 20, 2017), https://www.consumerreports.org/amazon/amazon-echo-voice-commands-offer-big-benefits-to-users-with-disabilities/.

[24] OrCam – See for Yourself, OR CAM, http://www.orcam.com/ (last visited Aug. 10, 2018).

[25] Global Initiative for Inclusive Information and Communication Technologies, Internet of Things: New promises for Persons with Disabilities (2015).

[26] For more information about the Uni, visit: http://www.motionsavvy.com/.

[27] *What is the Difference Between Accessible, Usable, and Universal Design?,* UNIVERSITY OF WASHINGTON (Sept. 15, 2017), https://www.washington.edu/doit/what-difference-between-accessible-usable-and-universal-design.

For companies, there is the potential to tap into the global elderly and disabled assistive devices market, which was valued at $14 billion in 2015 and is expected to surpass $26 billion by 2024.[28] Many IoT products designed for persons with disabilities have risen to mainstream popularity, and this translates to economic gains for many companies as well.[29]

However, unique privacy risks and challenges can be raised by the collection, use, and sharing of user data generated by these devices and services. Depending on the circumstances, privacy can be enhanced or diminished by IoT technologies, creating potential tensions between privacy gains and losses. How people address those tensions depends upon context—including how the service or device is used, who is using it, and individual preferences and values. Some members of the disability community may weigh benefits and privacy risks differently than others. This consideration—evaluating the ways IoT devices and services allow persons with disabilities to enhance their privacy vs. creating privacy risks via data collection—deserves more nuanced consideration and engagement by stakeholders – companies, users, advocates, policymakers, and others. The Fair Information Practice Principles provide a framework for recognizing and understanding the unique privacy considerations faced by the disability community when using IoT devices and services (See Table 1).

---

[28] TJ 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.

[29] Disability tech goes mainstream, Financial Times (Oct. 26, 2017), https://www.ft.com/content/ae91d600-8caf-11e7-9580-c651950d3672; How Tech for the Disabled Is Going Mainstream, Bloomberg Businessweek (Sept. 24. 2019), https://www.bloomberg.com/news/articles/2009-09-23/how-tech-for-the-disabled-is-going-mainstream.

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

FIPP	FIPP Description	Unique Impact on Persons with Disabilities	Example
Privacy Considerations: The Use of the IoT *by* Persons with Disabilities			
Transparency	Consumers have a right to easily understandable and accessible information about privacy and security practices.	Transparency mechanisms can exclude some persons with disabilities when 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 a user when the device is collecting audio data without providing other cues, such as auditory or tactical notifications.
Individual Control	Companies should provide users the right to control what personal data companies collect from them and how they use it.	Persons with disabilities are limited in their ability to choose amongst different IoT devices and services and to choose different data collection settings for a particular IoT device or service.	Smart TVs with microphones that require a button or remote 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* Persons with Disabilities			
Respect for Context	Companies should not collect, use, and disclose personal data in ways that are consistent with the context in which users provide the data.	Information collection, use, or disclosure may be more sensitive or revealing for persons with disabilities than for persons 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 have a different meaning for persons with disabilities than it does for persons without disabilities.	Browser fingerprinting technologies that collect information about a user's visit to a website can detect the use of assistive plugins, which can reveal a disability otherwise unobservable online.
Security	Consumers have a right to secure and responsible handling of personal data.	The consequences of IoT security failures may pose more serious outcomes or negative externalities for persons with disabilities than for persons 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 persons with disabilities.

Recommendations

With the FIPPs as a guide, and a firm understanding of the nuances of the unique privacy considerations of persons with disabilities, developers can protect the privacy of persons with disabilities. In order to address these privacy considerations, companies and IoT developers should:

1. **Include Persons with Disabilities in the Design of IoT Technologies**. Accessibility and the privacy of persons with disabilities should not be an afterthought for the IoT and new technology developers. The appropriate timing for integrating accessibility is at the earliest possible iteration of the technology.

2. **Promote Research**. In order to successfully build the IoT with universal or accessible design, research—both qualitative and quantitative—is needed to understand how persons with disabilities utilize the IoT and feel about the current privacy landscape of the IoT.

3. **Build Privacy by Design Approaches**. Companies should take into account the sensitive nature of the data collected from the IoT used by persons with disabilities and implement these considerations into the design of IoT products.

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

5. **Enhance Awareness of IoT Risks and Benefits.** Policymakers should consider the risks posed to all users of the IoT and data-reliant technologies, including not only the potential enhanced risks that persons with disabilities may face when using the IoT, but also the particularly high value that some of these very same technologies provide to those communities.

While it will take a combination of industry changes, research, and collaborations to address the privacy considerations faced by persons with disabilities when using the IoT, it is necessary that we begin recognizing the unique privacy considerations of persons with disabilities in the future of the IoT.