Comments from
THE FUTURE OF PRIVACY FORUM

to

NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
US DEPARTMENT OF COMMERCE
Washington, D.C.

Docket No. 160331306-6306-01:

The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things

John Verdi, Vice President of Policy
Chanda Marlowe, Intern
THE FUTURE OF PRIVACY FORUM[*†]
1400 I St. NW Ste. 450
Washington, DC 20005

www.fpf.org

June 2, 2016

[*] The Future of Privacy Forum (FPF) is a Washington, DC based think tank that seeks to advance responsible data practices by promoting privacy thought leadership and building consensus among privacy advocates, industry leaders, regulators, legislators and international representatives.
[†] The views herein do not necessarily reflect those of our members or our Advisory Board.

I. Executive Summary

The Future of Privacy Forum (FPF) appreciates the opportunity to provide these Comments in response to the NTIA's April 5, 2016 Request for Comment (RFC) on the benefits, challenges, and potential roles for the government in fostering the advancement 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 to consumers and to society of the inter-connected applications offered through the Internet of Things.[1] FPF also recognizes the privacy and security challenges presented by the Internet of Things as technology evolves. FPF has worked, from the beginning, to ensure that privacy and security are integrated into those implementations of the Internet of Things that involve the collection and sharing of personal information. Starting with our original project on the smart grid, an early white paper on Privacy by Design in the smart grid (jointly authored with Information and Privacy Commissioner of Ontario, Ann Cavoukian, Ph.D.),[2] and continuing to include our current work on "home devices,"[3] "wearables,"[4] "connected cars,"[5] "drones,"[6] and "smart stores,"[7] FPF has acquired experience and insights into the technologies and services associated with connected device ecosystems that we are pleased to share here.

FPF urges NTIA to consider:

- While many applications of the Internet of Things directly touch consumers and implicate privacy concerns, many applications have little or nothing to do with consumers and data privacy because they have no connection to an individual. For example, an oil company using sensors to monitor its Alaskan pipeline and a power generation company using sensors to predict and avoid potential failures are examples of machine-to-machine (M2M) connections that are not typically tied to individuals.

---

[1] 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-of-things-all-the-rage-at-consumer-electronics-show/.

[2] 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) [hereinafter *Smart Privacy for the Smart Grid*], *available at* http://www.ipc.on.ca/images/resources/pbd-smartpriv-smartgrid.pdf.

[3] Future of Privacy Forum, *Always On: Privacy Implications of Microphone-Enabled Devices* (2016) (hereinafter *Always On*), *available at* https://fpf.org/wp-content/uploads/2016/04/FPF_Always_On_WP.pdf.

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

[5] Future of Privacy Forum, *The Connected Car and Privacy, Navigating New Data Issues* (2014) [hereinafter *The Connected Car*], *available at* https://fpf.org/wp-content/uploads/FPF_Data-Collection-and-the-Connected-Car_November2014.pdf.

[6] 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/progress-on-drone-privacy-best-practices.

[7] 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/.

- The Internet of Things presents a major opportunity to support the use of data in ways that will benefit disadvantaged populations and promote inclusion.

- Privacy safeguards are important, but they should be carefully calibrated in light of emerging technologies, business practices, and consumer behavior.

- FPF's experiences working with Smart Grid technology – including FPF's "PrivacySmart" TRUSTed Smart Grid privacy seal – can serve as a useful example of how privacy and security can be integrated into the world of connected devices.

- Existing oversight mechanisms and privacy by design principles are well positioned to address many of the privacy concerns raised by the Internet of Things. Multistakeholder engagements may play a helpful role in focusing attention and resources on key issues (e.g. de-identification of IoT data), but the federal government should not pursue a legislative or regulatory agenda that targets IoT technologies, because a prescriptive, top-down approach would stifle meritorious, responsible uses of IoT technologies and data.

II. The Internet of Things & Privacy

Not all IoT capabilities implicate privacy concerns. While many applications of the Internet of Things directly touch consumers and implicate privacy concerns, many applications have little or nothing to do with consumers and data privacy because they have no conceivable connection to an individual.[8] An oil company using sensors to monitor its Alaskan pipeline and a power generation company using sensors to predict and avoid potential failures are examples of machine-to-machine (M2M) connections that are not tied to an individual.[9] It is important that the NTIA understand and distinguish between the consumer and non-consumer uses of connected devices to ensure that policies do not unduly impact industrial uses of connected devices.

Many IoT applications of the Internet of Things *do* involve consumers and consumer privacy. This connectivity can provide substantial benefits for research and analytics, and can be applied in multiple ways that will benefit society and individuals. From traffic management to healthcare improvements, there is a wide range of possible benefits that can be derived from information networks created by the Internet of Things. There is the potential to improve personal safety, improve public safety, increase consumer convenience, provide environmental benefits and promote business innovation. These benefits will occur when industry is able to layer applications on top of connected devices and create a network of smart systems.

Maximizing such benefits necessarily will require collecting, retaining, and sharing information in new ways. Information sharing on the scale required by the Internet of Things implicates

[8] Kishore Swaminathan, *Toasters, Refrigerators and the Internet of Things*, Accenture (Mar. 2012), http://www.accenture.com/us-en/outlook/Pages/outlook-journal-2012-toasters-refrigerators-internet-things.aspx.
[9] *Id.*; *see also 50 Sensor Applications for a Smarter World*, Libelium, http://www.libelium.com/top_50_iot_sensor_applications_ranking/ (last visited May 31, 2013).

privacy risks and security concerns that have not been traditionally associated with household items and vehicles.

If there are lax controls and insufficient oversight over the collection of personal information through connected devices, consumers will lose trust in the evolving technologies. Even with proper controls and oversight, helping consumers understand the benefits from these innovations and the protections in place is important lest they feel that personal control has been sacrificed for corporate gain.[10] With consumer trust in mind, European Commission Vice-President responsible for the EU Digital Agenda Neelie Kroes has cautioned that industry "cannot innovate in a bubble if citizens are not coming along for the journey."[11]

In short, business-developed standards designed to address security and privacy issues are needed to ensure that the Internet of Things achieves its full potential.[12]

The Fair Information Practice Principles (FIPPs) have long provided the foundation of consumer privacy protection in this country, and still embody core privacy values. However, the Internet of Things raises new issues around the FIPPs.

At their core, the FIPPs articulate basic protections for handling personal data: (1) Transparency, (2) Individual Control, (3) Respect for Context, (4) Security, (5) Access and Accuracy, (6) Focused Collection, and (7) Accountability.[13] Over time, as technologies and the global privacy context have changed, the FIPPs have been presented in different ways with different emphases.[14] The FIPPs are not meant to establish a rigid set of guidelines for the processing of information. Instead, they are designed to serve as high-level guidelines.

While the traditional mechanisms—such as presentations of detailed privacy policies and prompts for consents—have served to promote the FIPPs in many contexts, new mechanisms may be appropriate for some implementations of the Internet of Things.[15] Accordingly, we urge policymakers to enable the adaptation of these fundamental principles in ways that reflect

---

[10] *See generally* Jenifer S. Winter, Privacy and the Emerging Internet of Things: Using the Framework of Contextual Integrity to Inform Policy (2012), available at http://www.ptc.org/ptc12/images/papers/upload/PTC12_W1_Jenifer%20Winter%20(Paper).pdf (published in the Pacific Telecommunications Council Conference Proceedings 2012).

[11] Neelie Kroes, Vice-President of the European Commission responsible for the Digital Agenda, As the IoT Matures Into a Connected Society, Speech at the High-level Internet of Things Conference (May 16, 2011), available at http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=7008.

[12] *See Make IoT Reach its Full Potential: Why Businesses Need to Work Together*, MICROSOFT FOR WORK, (August 24, 2014), https://blogs.microsoft.com/work/2014/08/24/make-iot-reach-its-full-potential-why-businesses-need-to-work-together/#sm.000002fcrlcqv4fsex2xe579cjxxf.

[13] *See, e.g.*, The White House, *Consumer Data Privacy in a Networked World* (Feb. 2012); OECD, OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data 14 (2013), available at http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.

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

[15] *See* Fred H. Cate et al., Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines 7 (2013).

technological and market developments. New issues around the FIPPs can be addressed with openness to flexibility and new forms of notice.

III. The Internet of Things & Inclusion

In past papers,[16] we have discussed how traditional privacy principles can provide useful guidance when developing data practices on the Internet of Things and how new technologies require new implementation approaches or different applications of those underlying principles. Here, we would like to highlight inclusion-related benefits. As we add privacy restrictions, we want to support the use of data in ways that will benefit disadvantaged populations.

When the nonprofit Pew Research Center queried more than 1,600 experts on the subject, 83 percent predicted the Internet of Things will "have widespread and beneficial effects on the everyday lives of the public by 2025."[17] Among other advantages, IoT devices are widely expected to improve public health by keeping patients in closer touch with doctors, reduce highway deaths by automatically braking vehicles to avoid crashes, and boost food supplies by helping farmers tend their crops.

IoT can improve the day-to-day quality of life for citizens – even those who are not connected to the Internet, who don't know what IoT is, or who may not be able to afford IoT-enabled technology, including disadvantaged groups and rural communities. Specific examples are below.

For people who are visually impaired:

- the OrCam,[18] a wearable video camera that is designed for the visually impaired, translates text to audio in real time.
- dot, [19] the world's first braille smart watch, features a series of dull pins that rise and fall at customizable speeds and allows users to read text messages and e-books.
- cloud-connected insoles, developed at MIT Media Lab, work with a mobile device to help the user navigate a city without looking at a smartphone for directions.[20]
- home automation applications, like Nest, allow for easy control of appliances and the home thermostat, all with the touch of a button on a smart phone.[21]
- iRobot's Roomba,[22] a smart vacuum cleaner equipped with a system of software and sensors, can find its way around a home of any shape or size.

---

[16] *See, e.g.*, *Smart Privacy for the Smart Grid*, *supra* note 3; *Always On*, *supra* note 4; *The Connected Car*, *supra* note 6.

[17] Pew Research Center, *The Internet of Things Will Thrive by 2025* (2014), *available at* http://www.pewinternet.org/files/2014/05/PIP_Internet-of-things_0514142.pdf.

[18] *OrCam – See for Yourself*, OR CAM, http://www.orcam.com/ (last visited May 20, 2016).

[19] *The First Braille Smartwatch*, DOT, http://fingerson.strikingly.com (last visited May 20, 2016).

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

[21] *Nest app – Your Home in Your Hand*, NEST, https://nest.com/app/ (last visited May 20, 2016); Global Initiative for Inclusive Information and Communication Technologies, *Internet of Things: New promises for Persons with Disabilities* (2015).

For people with mobility-related disabilities:

- smart home technology allows users to control things in his or her home that may be physically difficult to reach, such as lights, door locks or security systems.[23]
- connected cars are an accessibility tool.[24]
- indoor location mapping will allow the user to immediately identify the location of various services, including ramps, accessible services, and escalators and elevators in public places.[25]

For people who are deaf or hard of hearing:

- Ring,[26] a connected doorbell and home security solution, alerts users to motion as soon as it's detected, so they can remotely monitor their door.

For older adults and the elderly:

- sensors from San Francisco-based Lively[27] alert relatives when an older family member fails to take medicine, eat or return home from a walk.

For those with health concerns:

- MedTronic's Continuous Glucose Monitoring, [28] a wearable device, displays a constant reading of a diabetic's blood glucose level. (A tiny electrode is inserted under the skin, which then transmits the glucose reading via wireless radio frequency to a display device.) Reports may be shared with parents, reducing risk of child death, and with care providers, leading to lower complications.
- Ralph Lauren's Polo Tech Shirt, [29] a shirt with conductive threads woven into it and a small snap-on module that weighs less than 1.5 ounces, relays information like heart rate and breathing data to a Bluetooth-connected iPhone or iPad.

For the infirm:

- General Electric (GE) Healthcare has developed technology to keep hospitals more sanitary and to reduce medical errors. GE's technology, for example, can determine whether soap and sanitizer dispensers are used by medical personnel before and after seeing a patient.[30]

---

[22] *Roomba – Your Partner for a Cleaner Home,* IROBOT, http://www.irobot.com (last visited May 20, 2016).
[23] Global Initiative for Inclusive Information and Communication Technologies, *Internet of Things: New promises for Persons with Disabilities* (2015).
[24] *Id.;* Paul Stenquist, *In Self-Driving Cars, a Potential Lifeline for the Disabled*, INTERNATIONAL NEW YORK TIMES (November 7, 2014), http://www.nytimes.com/2014/11/09/automobiles/in-self-driving-cars-a-potential-lifeline-for-the-disabled.html?_r=0.
[25] *Id.*
[26] *Never Miss a Visitor,* RING, https://ring.com (last visited May 20, 2016).
[27] *Lively 24/7 Emergency Medical Alert System,* LIVE!Y, http://www.mylively.com/how-it-works (last visited May 20, 2016).
[28] *Continuous Glucose Monitoring,* MEDTRONIC, http://www.medtronicdiabetes.com/products/continuous-glucose-monitoring (last visited May 20, 2016); Global Initiative for Inclusive Information and Communication Technologies, *Internet of Things: New promises for Persons with Disabilities* (2015).
[29] *The PoloTech Shirt*, RALPH LAUREN, http://press.ralphlauren.com/polotech/ (last visited May 20, 2016).
[30] *See GE Scientists Develop Multi-sensing Handheld Probe to Assess and Prevent Pressure Ulcer Formation During Hospital Stays,* GE GLOBAL RESEARCH (March 19, 2015), http://www.geglobalresearch.com/news/press-

- GE Healthcare technology can also track when patients get in and out of bed to help prevent falls, monitor clinical roundups to ensure that clinicians check in on patients at least once per hour, and revolutionize the protocol for preventing and treating painful pressure ulcers.[31]
- AiCure,[32] a company that combines video facial recognition and artificial intelligence, can help confirm that patients have taken their medication.

For the economically disadvantaged:

- smart meters offer access to detailed consumption data that can assist customers in managing their energy usage, which may save customers money on their energy bills.[33]
- M2M technology, integrated with new payment platforms, is expanding access to credit by enabling two new payment methods: pay-as-you-go ("PAYG") asset financing, which allows consumers to pay for products over time, and prepaid, where consumers pay for services on an as-needed basis.[34]

For farmers in rural communities:

- crop sensors can offer precise information about what amounts of fertilizers and pesticides are needed. This information can be fed directly into application machines that automatically dispense the correct amounts of each, which will save the farmer money.[35] sensors in the soil can also provide data for more efficient irrigation.[36] Hahn Family Wines, a family-owned winery based in the Santa Lucia Highlands in California's Monterey County, for example, "has launched a pilot project with Verizon that uses sensor data and analytics to conserve resources and add precision to watering and fertilizing five six-acre blocks at the company's 1,000-acre vineyard."[37]
- sensors embedded in equipment transmit real-time data and alert farmers to any needed maintenance before a breakdown occurs.[38]
- drones with optical and multi-spectral sensors allow farmers to gather vast amounts of data and remotely monitor the health of their crops. Using this data, farmers can easily assess crop conditions using the Normalized Difference Vegetation Index (NDVI), which has its roots in the space program and measures variances in vegetation.[39]

---

releases/ge-scientists-develop-multi-sensing-handheld-probe-to-assess-and-prevent-pressure-ulcer-formation-during-hospital-stays; *GE Healthcare and Summerville Medical Center Hail AgileTrac Success*, GE HEALTHCARE (April 12, 2013), http://newsroom.gehealthcare.com/ge-healthcare-and-summerville-medical-center-hail-agiletrac-success/.

[31] *Id.*

[32] *Do you know if your patients are taking their medicine? We do*, AICURE, https://www.aicure.com/.

[33] *Smart Privacy for the Smart Grid*, *supra* note 3.

[34] Pat Wilson & Stephanie Pow, Financial Inclusion and the Internet of Things: How Smart Machines Can Benefit the Poor, NEXT BILLION (August 4, 2015), http://nextbillion.net/financial-inclusion-and-the-internet-of-things/.

[35] Christopher Long, *Internet of Things Not Just for Cities*, NEXT BILLION (Nov. 10, 2015), http://www.govtech.com/fs/internet/Internet-of-Things-Not-Just-for-Cities.html.

[36] *Id.*

[37] Verizon, *State of the Market: Internet of Things 2016* (2016), http://www.verizon.com/about/sites/default/files/state-of-the-internet-of-things-market-report-2016.pdf

[38] Christopher Long, *Internet of Things Not Just for Cities*, NEXT BILLION (Nov. 10, 2015), http://www.govtech.com/fs/internet/Internet-of-Things-Not-Just-for-Cities.html.

[38] *Id.*

[39] *Id.*

drones mounted with thermal sensors can fly over herds of cattle and identify sick livestock by body temperature."[40]

IV. The Benefits and Challenges Posed by the Internet of Things

a. Smart Grid

FPF's experiences in working with Smart Grid technology show how privacy and security can become integrated into the world of connected devices.[41] Efforts are underway to modernize and make the current electrical grid "smarter" through the collection of data about consumer energy usage. Modernization will include new smart meters that can record detailed information about energy consumption, and smart appliances, such as thermostats, clothes washers, dryers, microwaves, hot water heaters, and refrigerators. Deploying these devices into households promises substantial benefits.

By themselves, smart meters offer access to detailed consumption data that can assist customers in managing their energy usage, which may save customers money on their energy bills. Smart meters provide greater efficiencies with regard to meter reading, faster handling of service orders, better management of outages, enhanced customer service capabilities, quicker resolution of billing issues, reduced meter tampering and better support for electric and plug-in hybrid electric vehicles. Smart meters also provide benefits beyond those measured at the individual and utility level. Society receives benefits from the more efficient operation of the electric grid, including reduced environmental impacts and reduced energy costs.

However, the collection, retention, and sharing of vast amount of data about individual energy consumption also comes with potential privacy risks. As noted above, together with Ann Cavoukian, Ph.D., Information and Privacy Commissioner of Ontario, FPF published a White Paper entitled *Smart Privacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation*.[42] In that paper, we noted that providing consumer access to energy-related information and offering dynamic pricing schemes based on individual energy use will "increase the level of personal information detail available as well as the instances of collection, use and disclosure of personal information."[43] As a result, electric utilities and ultimately other entities will gain access to information about what customers are using, when they are using it and what devices are involved. An individual's electricity usage profile could become a rich source of behavioral information on a granular level:

> Whether individuals tend to cook microwavable meals or meals on the stove; whether they have breakfast; the time at which individuals are at home; whether a house has an alarm system and how often it is activated; when occupants usually shower; when the TV and/or computer is on; whether appliances are in good condition; the number of gadgets in the home; if the home has a washer and dryer

[40] *Id.*
[41] *Smart Privacy for the Smart Grid*, *supra* note 3.
[42] *Id.*
[43] *Id.* at 9.

> and how often they are used; whether lights and appliances are used at odd hours, such as in the middle of the night; whether and how often exercise equipment such as a treadmill is used. Combined with other information, such as work location and hours, and whether one has children, one can see that assumptions may be derived from such information.[44]

This information, and the insights derived from it, can be used to the benefit of individuals and society. Or the information can be used in ways that raise concerns about individual privacy.

One of the key lessons FPF learned during our work on the smart grid was that there is great need for flexibility in determining how notice and consent mechanisms should be presented to consumers activating smart grid devices. These devices could be operated by mobile apps or come in the form of a smart thermostat or a transistor on the side of a hot water tank. Some state utility commissions thought that notice of data practices should be provided by requiring that consumers provide formal consent, sometimes even in notarized form, before enabling a device to access smart meter data held by the utilities. This consent mechanism would have proven burdensome for consumers who wanted to purchase and easily activate their equipment.

FPF convened the first smart grid privacy conference in Washington, D.C. and submitted comments on smart grid issues to the California, Colorado and Minnesota public utilities commissions. FPF supports creative approaches to the challenges raised by the smart grid.

To that end, FPF developed a first-of-its-kind privacy seal program powered by TRUSTe for companies providing services to consumers that rely on energy data.[45] The guidelines promote user control and rely upon the FTC's FIPPs.[46] FPF's "PrivacySmart" TRUSTed Smart Grid privacy seal requires that consumers provide affirmative consent to data practices, but the seal allows device providers flexibility to demonstrate that they are able to achieve this consent in meaningful ways.

The Department of Energy (DOE) has released a set of standards to guide privacy practices within the smart grid as well.[47] The purpose of the DOE Privacy Voluntary Code of Conduct (VCC) is to describe principles for voluntary adoption that

(1) encourage innovation while appropriately protecting the privacy and confidentiality of Customer Data and providing reliable, affordable electric and energy-related services;
(2) provide customers with appropriate access to their own Customer Data; and
(3) do not infringe on or supersede any law, regulation or governance by any applicable federal, state, or local regulatory authority.[48]

---

[44] *Id.* at 10-11.
[45] The Future of Privacy Forum and TRUSTe Launch a Smart Grid Privacy Seal Program, https://fpf.org/issues/smart-grid/.
[46] *Id.*
[47] United States Department of Energy, Data Privacy and the Smart Grid: A Voluntary Code of Conduct (2015), available at http://www.energy.gov/sites/prod/files/2015/01/f19/VCC%20Concepts%20and%20Principles%202015_01_08%20FINAL.pdf.
[48] *Id.*

The VCC's recommendations are intended to apply as high-level principles of conduct for both utilities and third parties and provide opportunities for new approaches to notice and consent.

b. Home Devices

One large challenge posed by the Internet of Things is that it introduces the possibility of collecting detailed information about our day-to-day activities within the most private of places—our homes.

Is your smart TV listening to your conversations? Are your children's toys spying on your family? These questions are being raised as the next generation of Internet-connected devices enters the market. Such devices, often dubbed "always on," include televisions, toys and home personal assistants, many of which now include microphones and speech-recognition capabilities.

One area FPF has focused on in particular is speech recognition technology. Speech recognition—the ability to speak naturally and contextually with a computer system in order to execute commands or dictate language—used to be considered a dream of science fiction. But over the last forty years, speech recognition technology has improved dramatically. Although the technology is far from perfect—the accuracy is diminished by background noise and recording quality, and certain accents are often more easily understood than others[49]—consumers in 2016 can now interact reasonably well via speech with a range of devices. This includes waking up and asking, "what's on my calendar?" to calibrating a connected thermostat, to dictating a text message or starting a browser search with the likes of "OK, Google," "Hey, Siri," "Hi Alexa," or "Hey, Cortana..."

The benefits of speech recognition technology are undeniable: hands-free control of technology improves the lives of people with physical disabilities, makes healthcare and other professional services more efficient through accurate voice dictation, enhances automobile safety, and makes everyday tasks more convenient.

A key feature is that by sending data to the cloud, where powerful computing can be applied, speech recognition services can improve over time. Making use of the huge advancements in data processing in recent years, voice-to-text technologies can now adapt to your speech patterns over time and are getting better at understanding speech in context. This aspect led early voice recognition pioneer Raj Reddy to predict that voice recognition technologies would pass the Turing Test in our lifetimes.[50]

The same feature of speech recognition technology that makes it useful—its ability to bring voice control into our everyday lives—is the feature that is now understandably raising privacy concerns, as microphone-enabled devices become integrated into our homes and daily environments.

---

[49] Speech recognition expert Marsal Gavaldà calls this diminished accuracy for children, seniors, and people with accents "the speech divide." CBC RADIO, *Here's why your phone can't understand your accent* (Sept. 13, 2015), http://www.cbc.ca/radio/spark/292-what-you-say-will-be-searched-why-recognition-sys- tems-don-t-recognize-accents-and-more-1.3211777/here-s-why-your-phone-can-t-understand-your-accent-1.3222569; *see also* Daniela Hernandez, FUSION, *How voice recognition systems discriminate against people with accents* (Aug. 21, 2015), http://fusion.net/story/181498/speech-recognition-ai-equality/.

[50] Xuedong Huang, James Baker & Raj Reddy, *A Historical Perspective of Speech Recognition*, COMMUNICATIONS OF THE ACM, Vol. 57 No.1, Pages 94-103, *available at* http://cacm.acm.org/magazines/2014/1/170863-a-historical-perspective-of-speech-recognition/abstract.

In a recent paper, *Always On: Privacy Implications of Microphone-Enabled Devices*,[51] FPF described three general categories of microphone-enabled devices, with some being capable of more than one function:

(1) Manually activated (requiring a press of a button, a flip of a switch, or other intentional physical action);
(2) Speech activated (requiring a spoken "wake phrase"); and
(3) Always on devices (devices, such as home security cameras, that are designed to constantly transmit data, including devices that "buffer" to allow the user to capture only the most recent period of time).[52]

Each category presents different privacy implications influenced in part by whether data is stored locally (an increasingly rare practice) or whether it is transmitted from the device to a third party or external cloud storage.

Manually activated speech recognition devices are straightforward: the user presses a button or flips a switch, and the microphone turns on and begins recording and transmitting audio to a voice-to-text translation service, often (but not always) resulting in text appearing simultaneously on the device.

In contrast, speech activated devices use the power of energy efficient processors to remain in an inert state of passive processing, or "listening," for a pre-set "wake phrase." The device buffers and re-records locally, without transmitting or storing any information, until it detects the word or phrase that triggers the device to begin actively recording.

When a modern smartphone is in a passive state (i.e. asleep, or with the microphone-enabled app in the background), the microphone can still internally (locally) process short stretches of audio, buffering and re-recording every few seconds to detect the device's wake phrase. In other words, it does not record or retain any audio data, or begin to transmit any data until it is "woken up." In this sense, then, it is not really "listening" to its environment, but instead utilizing the microphone as just another environmental sensor.

Finally, always on devices are those designed to record and transmit data all of the time. Most prominently, this includes home security cameras and baby monitors, but also includes a range of new devices. Cities can now detect gunfire via microphone networks, and there are microphones that can detect termite infestations by listening to audio outside of the range of the human ear.

These devices, because they are designed to be always on, evoke different privacy concerns from those that are manually or speech activated, and call for notice and consent frameworks in sync with the more extensive data collection that they enable.

Privacy implications will also vary by social and legal context. As discussed above, many devices dubbed "always on" are in fact only using the microphone to detect a wake phrase. However, the fact remains that microphones and specifically voice data retain unique social and

[51] *Always On*, *supra* note 4.
[52] *Id.*

legal significance. In some instances, laws that protect biometric information may apply. In general, sector-specific laws and regulations will also apply on the basis of the content of the voice communications.[53]

The collection of certain voice characteristics for the purpose of recognizing an individual, for example, implicates a range of laws. At the federal level, a "voice print" is considered either a biometric or personal record in the context of the Privacy Act,[54] FERPA,[55] and HIPAA,[56] and thus subjected to greater regulatory restrictions. Similarly, several states have expanded their legal definitions of personally identifiable information in certain identity theft or breach notification laws to include some form of biometrics.[57]

However, there is an important difference between speech recognition and voice recognition—the latter indicating biometric identification. The majority of speech-enabled devices on the market today are not designed for the purpose of uniquely identifying a person through the biometric characteristics of her voice. Instead, they aim to create products for which speech is a useful interface for engagement. In the future, however, it can be foreseen that unique voice recognition might become a useful consumer tool—for example, to permit only a specific person to access a device, or to enable parental controls by distinguishing between user accounts. Companies considering adding such features should be aware of the increasing number of federal and state laws regarding biometric identification.[58]

Moving forward it will be important to recognize that voice data is unique in its historical protection, communicative content, and biometric features. Useful guiding principles are beginning to emerge,[59] and the conversation will continue to evolve on this subject as social norms shift about when and where we should expect to be able to speak to our devices. In

---

[53] *E.g.* 18 U.S.C. § 2511 (prohibiting interception of oral communications).

[54] 22C.F.R.§308.3 ("Record means any document, collection, or grouping of information about an individual maintained by the agency, including but not limited to . . . any other personal information which contains . . . a finger or voiceprint.").

[55] 34 C.F.R.§99.3("Biometric record, as used in the definition of personally identifiable information, means a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual. Examples include . . . voiceprints").

[56] 45 C.F.R. § 164.514 (listing "[b]iometric identifiers, including finger and voice prints" as examples of personal information that must be removed from a data set before that data set can be considered properly de-identified and thus no longer subject to HIPAA regulations).

[57] *See, e.g.*, Conn. Gen.Stat.§38a-999b; IowaCode§715C.1; Neb.Rev.Stat.§87-802; N.C.Gen.Stat.§75 66; Or.Rev.Stat.§165.800; Or.Rev.Stat.§336.184 (regulating student educational records); Wis. Stat. § 943.201; Wyo. Stat. § 6-3-901.

[58] 22 C.F.R.§308.3 ("Record means any document, collection, or grouping of information about an individual maintained by the agency, including but not limited to . . . any other personal information which contains . . . a finger or voiceprint."); 34C.F.R.§99.3 ("Biometric record, as used in the definition of personally identifiable information means a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual. Examples include . . . voiceprints"); 45 C.F.R. § 164.514 (listing "[b]iometric identifiers, including finger and voice prints" as examples of personal information that must be removed from a data set before that data set can be considered properly de-identified and thus no longer subject to HIPAA regulations).

[59] *See* Alta Associates' Executive Women's Forum, *Voice Privacy Guiding Principles* (March 2016), http://c.ymcdn.com/sites/www.ewf-usa.com/resource/collection/CAA076AF-9566-4E1E-9F07-6421154DE0EA/Voice_Privacy_Guiding_Principles_Public_(final).pdf.

considering the benefits of speech-enabled devices in parallel to their legitimate privacy implications, forward-looking companies will be well-served to use the power of technology itself to enable the power of speech recognition while protecting consumer privacy and control.

c. Wearables

FPF is committed to supporting responsible privacy and security practices for wearable and mobile devices and related apps and services ("Wearables") that help users track physiological information hold the potential to greatly improve consumers' lives. Highlights of our efforts around consumer wellness data and wearables include public filings cited by the Federal Trade Commission on the benefits of the Internet of Things; *A Practical Privacy Paradigm for Wearables* whitepaper;[60] and an active working group promoting and developing best practices for consumer wearables.

Wearables deploy sensors to collect environmental, behavioral, and social data for and from their users. Consumer-generated data from these devices is already generating substantial benefits for users, helping individuals manage their fitness, exercise, and biofeedback; improving personal productivity and efficiency; and making other technologies simpler and easier to use. Research based on data collected by wearables could reveal insights that could provide broad societal benefits.

This same data, if not properly protected, or if used in unethical or illegal ways, could be used to put individuals' privacy at risk. Critics worry that users could find themselves unfairly discriminated against by employers or insurers on the basis of their self-generated information, or have their reputations damaged or their safety put at risk by a data breach.

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

It is important to note that in many areas data collected by wearables is also subject to other legal protections. In the U.S., this includes sector-specific legislation such as COPPA, FCRA, or the ADA, as well as federal and state laws governing insurance and illegal discrimination.[61] In many cases, personal wellness information is covered by the Health Insurance Portability and Accountability Act (HIPAA), which imposes certain privacy and security requirements on healthcare providers and their business associates. Medical devices that can be worn or carried like a consumer wearable are also regulated for safety by the FDA.

---

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

[61] *See, e.g.*, FPF List of Federal Anti-Discrimination Laws, FUTURE OF PRIVACY.ORG, http://www.futureofprivacy.org/fpf-list-of-federal-anti-discrimination-laws/.

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

In Europe and other jurisdictions, national (and soon EU-wide) privacy laws also set baseline privacy and security expectations. While such laws provide the starting point for data protection, they often also impose higher standards on personal information that is considered especially sensitive, such health or financial data. In some cases, consumer-generated wellness data is likely to fall within such protected categories. The European Data Protection Supervisor, for example, has noted that "Lifestyle and well-being data will, in general, be considered [sensitive] health data, when they are processed in a medical context…or where information regarding an individual's health may reasonably be inferred from the data (in itself, or combined with other information), especially when the purpose of the application is to monitor the health or well-being of the individual (whether in a medical context or otherwise)."[62] Where lifestyle or wellness data *is* considered sensitive, additional restrictions on data processing are imposed.

As the Article 29 Working Party has noted, however, "On the other side of the spectrum . . . there is a category of personal data generated by lifestyle apps and devices that is, in general, not to be regarded as [sensitive] health data."[63] There are also some apps and devices where "it is not obvious at first sight whether or not the processing of these data should qualify as the processing of health data."[64] It is important to distinguish between personal data that are, on the one hand, clearly akin to medical information which reveal inherently sensitive details about an individual's health status and, on the other hand, those raw or low-impact personal data that do not expose an individual's private health information, especially given that most commercial wearable apps and devices exist in a grey zone between these poles.

Given the lack of bright lines between sensitive health and non-sensitive lifestyle data, treating all health-related personal data the same would be a mistake. The stringent privacy, security, and safety requirements appropriate for medical devices and medical data would render many

[62] European Data Protection Supervisor, Opinion 1/2015 Mobile Health: Reconciling Technological Innovation with Data Protection (May 21, 2015), https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-05-21_Mhealth_EN.pdf.

[63] As the Article 29 Working Party noted, "there is a category of personal data generated by lifestyle apps and devices that is, in general, not to be regarded as health data within the meaning of Article 8. This concerns data from which no conclusions can be reasonably drawn about the health status of a data subject." *See* Article 29 Working Party, Letter, *Annex – health data in apps and devices* (Feb. 5, 2015), http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf.

[64] *Id.*

commercial fitness devices impractical for everyday consumers. At the same time, it would be a mistake to treat wellness data as if it were generic personal information without any sensitivity.

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

In determining where data fall on this spectrum, some relevant factors to consider would include: the context and purpose for which data are collected and used; whether data are inherently/clearly medical data; whether the data is made available to a member of the medical community; whether there is a clear and close link between the data and a user's health status; whether data is used to measure or predict health risks and/or to enable medical follow-up; whether conclusions are or can be reasonably drawn about the health status of a user based on the data; the compatibility of the use; and the existence of appropriate safeguards.[65]

Practical guidance that can be further tailored to meet local requirements can build upon existing legal expectations. Apps and devices that capture other personally identifiable information should look to existing best practices and guidance documents, such as the FTC *Internet of Things Report*,[66] the Article 29 Working Party *Opinion on the Recent Developments on the Internet of Things*,[67] or the FPF-CDT *Best Practices for Mobile Application Developers.*[68] FPF supports a baseline of responsible practices intended to support a targeted FIPPs-based trust framework for the collection and use of consumer-generated wellness data.

[65] *See* Article 29 Working Party, Letter, *Annex – health data in apps and devices* (Feb. 5, 2015), http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf.
[66] FTC Staff Report, Internet of Things: Privacy & Security in a Connected World (Nov. 2013), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.
[67] Article 29 Working Party, Opinion 8/2014 on the Recent Developments on the Internet of Things (Sept. 16, 2014), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.
[68] Future of Privacy Forum & the Center for Democracy & Technology, *Best Practices for Mobile Application Developers* (Dec. 2011), https://www.cdt.org/files/pdfs/Best-Practices-Mobile-App-Developers.pdf.

d. Connected Cars

The connected car refers to the use of in-car telematics, a range of technologies that leverage connectivity, whether over the Internet or via dedicated short-range communications (DSRC), with diagnostic, location, or other information to provide new safety, convenience, and communications services. Connectivity has the further potential to reduce traffic congestion, reducing both vehicle emissions and energy consumption. Some common telematics services already available in vehicles include crisis and crash assistance, destination information and guidance, emergency services, remote monitoring, and a variety of vehicle alerts, news, and infotainment.[69] The precise definition of the "connected car" is evolving rapidly as vehicles are outfitted with new technologies. According to the Department of Transportation, connectivity promises to allow an elaborate network of communications among vehicles, infrastructure, and any wireless device inside the vehicle.[70]

Connectivity leverages data collected both inside and outside of the car to provide a variety of new driving benefits, conveniences, and consumer applications. According to former Transportation Secretary Ray LaHood, connectivity offers tremendous promise for improving safety, reducing traffic congestion, and increasing fuel efficiency.[71]

Our paper, *The Connected Car and Privacy: Navigating New Data Issues*,[72] provides an overview of the various technologies currently available in cars. As explained below, connected cars offer safety features, environmental benefits, and convenience.

Safety features. Connectivity can take advantage of both location and diagnostic information to assist in emergency response. For example, the OnStar service provides automatic crash response, which allows an equipped-vehicle to alert emergency responders in the event of an accident, such as when an airbag deploys, and allows roadside assistance services to pinpoint the location of a car.[73] These sorts of features will become more commonplace in vehicles, but connectivity will also allow drivers to receive location-based warnings and information about weather emergencies or road conditions.

With connectivity, diagnostic and vehicle performance information generated by a car can be used by manufacturers, technicians, and drivers to get feedback about how vehicles are performing on the road. For the first time, this type of information can be sent to vehicle manufacturers who can chart vehicle performance in order to plan safety and performance improvements in the future, which could be immensely beneficial. Connectivity can also

---

[69] Edmunds, Telematics Chart, http://www.edmunds.com/car-technology/telematics.html (last visited Oct. 1, 2014).
[70] U.S. Department of Transportation, Research and Innovative Technology Administration, Connected Vehicle Research in the United States, http://www.its.dot.gov/connected_vehicle/connected_vehicle_research.htm (last updated June 26, 2014).
[71] Press Release, New DOT Research Shows Drivers Support Connected Vehicle Technology, Appreciate Potential Safety Benefits, National Highway Traffic Safety Administration (May 22, 2012), http://www.nhtsa.gov/About+NHTSA/Press+Releases/2012/New+DOT+Research+Shows+Drivers+Support+Connected+Vehicle+Technology,+Appreciate+Potential+Safety+Benefits.
[72] Future of Privacy Forum, The Connected Car and Privacy: Navigating New Data Issues (2014), *available at* https://fpf.org/wp-content/uploads/FPF_Data-Collection-and-the-Connected-Car_November2014.pdf.
[73] SOS Emergency, OnStar, https://www.onstar.com/web/portal/emergencyexplore?g=1 (last visited Oct. 1, 2014).

improve use-based insurance implementation, subject to state insurance laws. Instead of needing a separate device, consumers will be able to directly opt-in to use-based insurance by sharing information from the vehicle directly with insurance companies.

Environmental Benefits. In addition to safety benefits, connectivity will allow for continuous emissions testing of vehicles, which could reduce oil consumption by 4% nationwide, saving six billion gallons of gasoline.[74] Services like Automatic can monitor driver behavior, nudging drivers towards better and more fuel-efficient behaviors, and provide an interactive driving score.

Optimizing traffic times will improve fuel-efficiency, and eventually, the ability of vehicles to communicate with traffic signals will help to eliminate unnecessary stops and allow drivers to operate their vehicles at optimal fuel-efficiency. And at a macro level, city planners and transportation agencies will be able to use real-time traffic data and aggregated driver information to optimize traffic flows and even target roads most in need of repair.

Convenience. Connectivity can also power a range of consumer applications to make driving more convenient and more fun. Other remote monitoring services let drivers know if they should engage their parking brake, get fuel, inflate their tires, or get an oil change just from looking at an app on their smartphone. Applications also allow drivers to remotely start their cars and beat the heat (or the cold) by setting the car's internal temperature without even going outside, and to find their vehicles via their mobile phone in a crowded mall parking lot.

Our whitepaper on *The Connected Car and Privacy*[75] also describes the types of data collected and the purposes for which it is collected.

Geolocation Information. Connectivity provides consumers with more and more opportunities to take advantage of location-based services in their cars and real-time traffic-based navigation. In-car location-based services have long existed through personal GPS units and navigation apps in smartphones, but connected cars promise both to expand on these technologies and to include more location-based services through telematics technologies embedded in the connected car itself.

A vehicle's location can be determined through a variety of different methods, including cell tower signal-based technologies, Wi-Fi access points, crowd-sourced positioning, and GPS technology. Currently, some combination of GPS and onboard sensors allows for connected cars to be aware of the vehicle's physical location.

Similarly, onboard sensors can also be used to gather information about the car's immediate surroundings, detecting lane markings and obstacles alike. Three key technologies that rely on this external environmental information are blind spot detection systems, lane-departure warnings, and rear-parking detection.

---

[74] The Connected Car, Verizon Telematics, https://verizontelematics.com/pp/whitepapers/emissionswp.php (last visited Oct. 1, 2014).

[75] *The Connected Car*, *supra* note 6.

Cameras and sensors can be arrayed in various positions around a vehicle to provide 360 degree electronic coverage of the car's surroundings. For example, blind spot detection systems use ultrasonic or radar sensors on the side or rear of the vehicle to monitor traffic, while lane detection systems may use forward-facing cameras to identify lane markings. Parking detection systems can rely on both cameras and sensors that judge how close the vehicle is to nearby objects. Pairing these different sensors and cameras together can provide sophisticated obstacle avoidance systems that portend the future of automated driving.

Biometrics Information. In addition to external sensors, internal sensors that obtain information about the physical or biological characteristics and traits of a driver, or biometrics, will present opportunities for new vehicle features in the future such as providing access controls or driver identification. Biometric collection in cars involves collecting physical data such as facial recognition, vital signs, or voice samples. For example, voice recognition can be used to provide a hands-free experience for using applications in a connected car. Biometrics information could serve as powerful anti-theft protection, as well as providing increased safety and comfort inside the vehicle.

In the future, cars will be able to use internal cameras and sensors to automatically identify drivers. Vehicles will be able to quickly change car settings to accommodate different driving styles or driver profiles, such as for teenagers or the elderly. Additional sensors will augment these capabilities by collecting additional biometric data.

Automakers are engaged in research on biometric data, which can be collected in the car to provide real-time health monitoring for drivers. Conductive sensors in the steering wheel can monitor the driver's pulse and temperature. Sensors in the seatbelt can monitor breathing patterns.

This sort of biometric collection can provide a number of safety benefits for drivers with health conditions, as well as help drivers monitor their stress and help prevent crashes.

Behavioral Information. In addition to gauging the physical characteristics of the driver, vehicles will also become better attuned at responding to driver behavior. In-car technologies can gather information about the driver's attention, speed, steering and braking habits and combine this with other diagnostic data to provide new safety features. For example, one automaker's "Attention Assist" feature gathers over seventy different parameters within minutes of starting a vehicle in order to help the vehicle detect signs of driver drowsiness. It evaluates steering corrections along with other factors such as crosswinds, road surface quality, and how often the driver is engaging with the wheel to predict whether drivers are showing signs of fatigue, in which case it sounds an alert to the driver.

As stress and fatigue mounts, connected car safety systems could reduce driver distraction by automatically turning off the radio, blocking incoming cellphone calls, or bring the car to a stop in the event of a heart attack. Carmakers and federal safety regulators are also working on in-vehicle systems that could reliably detect when someone is too drunk to drive.

Subscriber & Registration. Many new telematics services will require user activation and on-going user accounts. Agreements to use these services will require personal information such as the user's name, address, and billing information to be collected from users. Some of this information may not have previously been collected by automakers. Because of the traditional relationship between vehicle manufacturers and car dealers, automakers generally lack a direct relationship with drivers. As a result, the collection of consumer subscriber information may involve a new set of data collection for automakers, even if subscriber or registration agreements are not a novel form of data.

Vehicle-to-Vehicle Communication. In the future, connected cars will expand their ability to sense, connect, and interact with the outside world, including other vehicles and their immediate environment. Dedicated short-range communications (DSRC) is a short-range automotive communication protocol used to facilitate this connectivity. While standards are still being developed, DSRC can be used not just in vehicle-to-vehicle (V2V) communication but also vehicle-to-infrastructure (V2I) communication to establish ad hoc networks. Whenever any connected car comes into communications range with a smart stoplight, other intelligent infrastructure, or another vehicle with DSRC, they will be able to form a network.

This constant broadcast and reception of vehicle information gives connected cars a 360 degree awareness of their outside environment. Each vehicle connected to the network will know the position, speed, and direction of every other nearby vehicle. Ultimately, V2V communications will enable vehicles to sense hazards on the road and issue warnings directly to drivers, allowing them to take actions to avoid or mitigate crashes.

According to a study by the National Highway Traffic Safety Administration (NHTSA), advance warnings through V2V could prevent up to 592,000 crashes and save 1,083 lives each year. V2V communications are anonymous and do not contain any specific location data linked to the driver themselves; instead, the only information shared is the car's relative position in terms of other vehicles.

This sort of external environmental information will eventually allow vehicles to cooperate with each other to ease traffic flow, protect pedestrians through DSRC-equipped smartphones, and help traffic agencies monitor and direct traffic flows. But DSRC can also be used to provide drivers with real-time monitoring of adverse weather conditions on the road. For example, cars that experience a loss of traction or begin hydroplaning can immediately send warnings to other cars in the area.

Each model year brings cars that are getting smarter and more connected, offering new safety features and consumer conveniences. By the end of the decade, one in five vehicles on the road will be connected to the Internet. But for consumers to welcome these advances, they need to be sure their personal data will be handled in a trustworthy manner, as early research shows that considerable numbers of new car buyers are concerned about data privacy when it comes to car connectivity.[76]

[76] *What's Driving the Connected Car*, MCKINSEY&COMPANY, (September 2014) http://www.mckinsey.com/industries/automotive-and-assembly/our-insights/whats-driving-the-connected-car.

To address those concerns, the Alliance of Automobile Manufacturers and the Association of Global Automakers have come together to put forward a set of privacy principles[77] for vehicle technologies and services. These privacy principles set a responsible course for new uses of connected car data and should help avoid any privacy bumps in the road.

The principles cover a wide variety of vehicular data, and they directly address some of the chief privacy concerns raised by new in-car technologies. For example, they cover location information, driver biometrics, and other driver behavioral data, such as seatbelt use or frequency of hard-breaking, that can be gathered by a vehicle, and require opt-in consent by consumers before any of this sensitive information can be used for marketing purposes or otherwise shared with independent third parties.[78] The principles also include a warrant requirement for geolocation information to be shared with law enforcement, absent exigent circumstances or certain statutory authorities.[79] These are important protections, and essential to ensure consumer data is being handled in a trustworthy matter inside the connected car.

e. Drones

The benefits of commercial and private drones, otherwise known as unmanned aircraft systems (UAS), are substantial. Technology has moved forward rapidly, and what used to be considered toys are quickly becoming powerful commercial tools that can provide enormous benefits in terms of safety and efficiency. UAS integration will have a significant positive economic impact in the United States. Whether UAS are performing search and rescue missions, helping farmers grow better crops in a more sustainable manner, inspecting power lines and cell towers, gathering news and enhancing the public's access to information, performing aerial photography to sell real estate and provide insurance services, surveying and mapping areas for public policy, delivering medicine to rural locations, providing wireless internet, enhancing construction site safety, or more—society is only just beginning to realize the full potential of UAS. UAS technology is already bringing substantial benefits to people's daily lives, including cheaper goods, innovative services, safer infrastructure, recreational uses, and greater economic activity. Inevitably, creative minds will devise many more UAS uses that will save lives, save money and make our society more productive.

However, the very characteristics that make UAS so promising for commercial and non-commercial uses, including their small size, maneuverability and capacity to carry various kinds of recording or sensory devices, can raise privacy concerns. As a result, individuals may be apprehensive about the adoption of this technology into everyday life. In order to ensure that UAS and the exciting possibilities that come with them live up to their full potential, operators should use this technology in a responsible, ethical, and respectful way. This should include a commitment to transparency, privacy and accountability.

---

[77] *Automakers Believe That Strong Consumer Data Privacy Protections are Essential to Maintaining the Trust of Our Customers,* AUTO ALLIANCE, http://www.autoalliance.org/auto-issues/automotive-privacy.
[78] *Id.*
[79] *Id.*

The NTIA launched the multistakeholder process on drones in 2015, bringing together a diverse group to find workable solutions to the privacy, transparency, and accountability issues regarding commercial and private use of drones. The group recently agreed on a set of best practices supported by key stakeholders including FPF, Amazon, the Association for Unmanned Vehicle Systems International, the Consumer Technology Association, CTIA – the Wireless Association, New America's Open Technology Institute, PrecisionHawk, the Small UAV Coalition, and X (formerly Google[x]).[80]

The best practices are intended to encourage operators to use UAS technology in a responsible, ethical, and respectful way. They provide enough flexibility to support innovative uses of this emerging technology, but at the same time provide firm privacy standards. The best practices acknowledge that the principles are qualified by the understanding that they are to be implemented as "reasonable" and "practical" – in order to allow flexibility for smaller operators, hobbyists or circumstances where compliance would be impractical. FPF has created an easy to read summary of these best practices to help educate drone operators. They are listed below:

1. Provide a privacy policy if you anticipate that you may collect personal information.
2. When persons have a reasonable expectation of privacy, do not intentionally collect personal information unless you have permission or a compelling reason to do so.
3. Avoid persistent and continuous collection of personal information, unless you have permission or a compelling reason to do so.
4. Minimize flying over private property, unless it impedes the purpose for which the drone is used, or you have permission, or legal authority.
5. Delete or de-identify personal information no longer needed for purposes explained in your privacy policy, unless you have permission to keep it longer or special circumstances exist.
6. Establish a process by which persons can request deletion of their personal data or communicate privacy and security concerns.
7. Do not use personal information for employment eligibility, promotion, or retention; credit eligibility; or health care treatment eligibility other than when expressly permitted by and subject to the requirements of a sector-specific regulatory framework or with consent.
8. Do not use or share personal information for any purpose that is not included in your privacy policy.
9. Unless you obtain permission, do not knowingly make personal information public, except if necessary to fulfill the purpose for which the drone is used.

[80] National Telecommunications and Information Administration, *Voluntary Best Practices for UAS Privacy, Transparency, and Accountability* (2016), *available at* https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-unmanned-aircraft-systems.

10. Do not use or share personal information for marketing purposes without first gaining permission.[81]

FPF's summary of the NTIA's Best Practices for Drone Use highlights measures that drone operators should take to manage security risks to personal information as well, including implementing a program that contains reasonable administrative, technical, and physical safeguards appropriate to the operator's size and complexity, the nature and scope of its activities, and the sensitivity of the covered data.[82]

f. Mobile Location Analytics (MLA)

Increasingly, the mobile advertising space and location technologies are at the forefront of innovative new consumer offerings and emerging privacy questions about how to appropriately handle consumer data. It is not surprising that complex tracking and audience measurement technologies can raise both consumer concerns and regulator interest.

New technologies, which rely on the fact that most people carry a mobile device, now allow venues such as airports, stores, and hotels to receive signals from devices that are in or near them. Mobile Location Analytics (MLA) provides technological solutions for Retailers by developing aggregate reports used to reduce waiting times at checkout, to optimize store layouts and to understand consumer-shopping patterns. The reports are generated by recognizing the Wi-Fi or Bluetooth MAC addresses of cellphones as they interact with store Wi-Fi networks.

Given the potential benefits that Mobile Location Analytics may provide to businesses and consumers, it is important that these practices are subject to privacy controls and are used responsibly to improve the consumer shopping experience. FPF worked with a group of MLA companies and Senator Chuck Schumer to create a Mobile Location Analytics Code of Conduct to provide an enforceable, self-regulatory framework for retail tracking.[83] The Code puts guidelines in place to create best practices that provide transparency and choice for consumers.

Under the Code, companies that collect data through this technology must limit how the information is used and shared and how long it may be retained. The Code mandates that companies de-identify the data and explain in their privacy policy how they do so. Companies are required to get opt-in consent when personal information is collected, or when a consumer will be contacted. The Code calls for opt-out consent where the information collected is not personal. In addition, this data cannot be collected or used in an adverse manner for employment, health care or insurance purposes. The standards put forth in the Code ensure that consumers understand the benefit of the bargain and have choices about how their information is used while allowing technology to continue to improve the shopping experience.

---

[81] Future of Privacy Forum, *Best Practices for Drone Use* (2016), *available at* https://fpf.org/wp-content/uploads/2016/05/FINAL-Drone-Graphic.pdf.
[82] *Id.*
[83] Press Release, The Future of Privacy Forum and Sen. Schumer Announce Important Agreement to Ensure Consumers Have Opportunity to "Opt-Out" Before Stores Can Track Their Movement via Their Mobile Devices (Oct. 22, 2013), *available at* http://www.futureofprivacy.org/2013/10/22/schumer-and-tech-companies-announce-important-agreement-to-ensure-consumers-have-opportunity-to-opt-out-before-stores-can-track-their-movement-via-their-cell-phones/.

V. The Future of Notice

It will not always be practical in the Internet of Things to address the collection and use of personal information via traditional notice and choice mechanisms. As pointed out in our White Paper,[84] some connected devices will not have screens or interfaces that readily present privacy notices or allow consumers to select among data practices.

Those responsible for implementing connected devices should provide notice that is tailored to the nature of the devices, the environments in which the devices will be used, the types of data to be collected and the data's intended use. Many IoT devices are beginning to provide notice of data collection through visual, auditory or tactile cues.

Amazon Echo, for example, uses a light ring to visually communicate its status with you. When the light ring is solid blue, the device is listening to you. [85] When all lights are off, the device is active and waiting for your request.[86] The solid red light indicates you have turned off the microphones on your device.[87] Those who want to know more about the Echo's privacy policy can actually ask, "Alexa, are you spying on me?" In response you will hear, "I only send audio back to Amazon when I hear you say the 'wake word.' For more information and to view Amazon's privacy notice, visit the help section of your Alexa app."

Your smartphone visually communicates with you by displaying small symbols (called glyphs) to let you know when a feature on the device is turned on or being used. The arrow glyph is now a widespread indication to users that their location information is being collected. iPhone users, for example, can click the arrow glyph to see which apps are using location services or check for arrows displayed to right of app names in System Preferences to see if an app has requested their location information in the last 24 hours.[88]

FPF's MLA Code[89] encourages MLA companies that track shoppers' locations through stores to develop privacy notice that inform consumers about how information will be collected, used, and stored as well. Signage is one way MLA companies are alerting consumers to the use of tracking technologies and directing consumers to where they can obtain more information. FPF has created model signage, which can be found at smart-places.org.[90]

[84] Christopher Wolf & Jules Polonetsky, *An Updated Privacy Paradigm for the "Internet of Things"* (2013).
[85] *Alexa and Alexa Device FAQs*, AMAZON.COM, http://www.amazon.com/gp/help/customer/display.html?nodeId=201602230
[86] *Id.*
[87] *Id.*
[88] *About Location Services in OS X and Safari*, APPLE INC., https://support.apple.com/en-us/HT204690
[89] Future of Privacy Forum, *Mobile Location Analytics Code* (2013), https://fpf.org/wp-content/uploads/10.22.13-FINAL-MLA-Code.pdf.
[90] *Mobile Analytics Opt Out*, FUTURE OF PRIVACY FORUM, http://smart-places.org/.