BEFORE THE UNITED STATES FEDERAL TRADE COMMISSION

WASHINGTON, DC

COMMENTS OF THE FUTURE OF PRIVACY FORUM ON CONNECTED SMART TECHNOLOGIES IN ADVANCE OF THE FTC "INTERNET OF THINGS" WORKSHOP	)

I. Introduction

On April 17, 2013, the FTC announced a Workshop to be held on November 21, 2013 to examine the privacy and security issues associated with connected "smart technologies," collectively referred to as the "Internet of Things."[1] The Future of Privacy Forum ("FPF")[2] appreciates this opportunity to provide these Comments on ways to address those privacy and security issues, and to do so, as the Commission has requested, in the context of the societal, economic and personal benefits of the Internet of Things and its new uses of data.

[1] FTC News Release, FTC Seeks Input on Privacy and Security Implications of the Internet of Things (Apr. 17, 2013), *available at* http://www.ftc.gov/opa/2013/04/internetthings.shtm.

[2] The Future of Privacy Forum is a Washington, D.C.-based think tank whose mission is to advance privacy for people in practical ways that allow for innovation and responsible use of data. The FPF Advisory Board includes privacy professionals, privacy scholars and academics. The co-chairs of FPF are Jules Polonetsky, its Executive Director, and Christopher Wolf, who leads the global privacy practice at Hogan Lovells US LLP.

The Internet of Things has been a focus of FPFs work since our founding in 2008. Starting with our original and still-ongoing project on the Smart Grid (and an early White Paper on Privacy by Design in the Smart Grid jointly authored with Information and Privacy Commissioner of Ontario, Ann Cavoukian,[3] Ph.D.) and continuing to include our current work on "Connected Cars" and "Smart Stores", FPF has acquired insights that it is pleased to share here.

The collection, analysis and use of personal data involved with connected smart devices provide many benefits, and privacy often is provided through transparency and accountability. Codes of conduct, seals and other public-facing and enforceable commitments are examples of how to address the privacy issues in the Internet of Things. In circumstances where the Fair Information Practice Principles (FIPPs) of timely notice and choice may not be available (for example, where the smart device interaction does not involve a screen or human activation), new ways to protect consumers need to be explored.

At the same time, care must be taken not to impose new modes of regulation on technologies simply because they are used in the Internet of Things. Fair Information Practice Principles still are germane even if their adaptability is unique. Promotion of leading practices is appropriate. Regulation can and should be technology neutral. And the Commission's prohibitions under Section 5 of the FTC Act against deceptive and unfair practices apply with full force.

The Internet of Things will continue to make beneficial uses of data possible, but only if practical privacy protections are in place to help promote consumer trust.

FPF commends the Commission for providing a forum where the privacy and security challenges presented by the Internet of Things can be explored.

[3] 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.

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

The "Internet of Things" is commonly understood to refer to the growing network of devices that capture, share and use data, including data about who we are and what we do.[4] In the Internet of Things, information networks are created through wired and wireless communications technologies embedded in physical objects.[5]

Providing context for a discussion of privacy and the Internet of Things, the Chief Scientist of Accenture has explained:

> [M]ost applications of [Internet of Things] will have little or nothing to do with consumers and data privacy. An oil company using sensors to monitor its Alaskan pipeline or a kennel club using RFID tags to locate lost canines or a power generation company using sensors on its turbines to predict and avoid potential failures—all applications in operation today—do not fall within the purview of regulations or data privacy concerns.[6]

But many applications of the Internet of Things *do* involve consumers and consumer privacy. A simple illustration is the car service UBER that uses mobile apps with geolocation and mapping capabilities to connect available taxis and car services with nearby passengers who have registered their payment card details. The service facilitates "on demand" transportation services with billing and payment pre-arranged.[7]

By 2015, 25 billion devices are projected to be connected to the Internet; this number could double to 50 billion devices by the end of the decade.[8] While mobile devices, such as those used for the UBER service, make up the majority of today's connected devices, the growth of

---

[4] Bill Wasik, *Welcome to the Programmable World*, Wired (May 14, 2013), http://www.wired.com/gadgetlab/2013/05/internet-of-things/.

[5] Michael Chui et al., *The Internet of Things*, McKinsey Quarterly (Mar. 2010), *available at* http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_internet_of_things.

[6] 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; *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).

[7] UBER has strict, published (and under Section 5 of the FTC Act, enforceable) privacy limits on how the information is used and shared. https://www.uber.com/legal/privacy.

[8] Dave Evans (CISCO), *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything* 3 (2011), *available at* http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

machine-to-machine (M2M) connections is expected to make up an increasing percentage of the connected devices market.[9] One scenario: Traffic signal adjustments will be made on the basis of speed and location data communicated by cars on local highways and roads. Another application: A medical device being used by a patient will be monitored in real time by a remote computer and doctors (or family) can be alerted if there is a problem, without human intervention. According to one survey, the M2M market will expand to 24 billion smart sensors by 2020 and will be worth approximately $1.2 trillion.[10]

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. Connected devices will communicate with each other, use sensors to observe external conditions, and access and analyze external sources of information, such as historical data:

> Imagine a portfolio of household good products – your laundry detergent and your dishwater – communicating with you to give a personal record that can help reduce water and energy use. Or imagine medical devices like glucose monitors that come with dietary advice and medicines that provide online side-effect alerts and tests. Or wine and spirits bottles that provide not just terroir history and cocktail tips but also personalized healthy drinking advice.[11]

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

---

[9] Machina Research, *The Connected Life: A USD4.5 trillion global impact in 2020* (Feb. 2012), *available at* http://connectedlife.gsma.com/wp-content/uploads/2012/02/Global_Impact_2012.pdf.

[10] Laurence Cruz, *Securing the Internet of Things*, CISCO (Mar. 24, 2013), http://newsroom.cisco.com/feature-content?type=webcontent&articleId=1158640.

[11] Matthew Yeomans, *The Internet of Things: How Connected Devices Can Drive Sustainability*, Guardian, (June 21, 2012), http://www.guardian.co.uk/sustainable-business/internet-of-things-connected-devices.

items and vehicles. Technologist Bruce Schneier has cautioned that the Internet of Things will give "eyes and ears" to businesses in new and unprecedented ways.[12]

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.[13] (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."[14])

In short, business standards designed to address security and privacy issues are needed to ensure that the Internet of Things achieves its full potential.[15]

III. The Privacy Challenges of the Internet of Things

Given the multiple inputs from sensors, geolocation technologies, collections of personal information and historical data, the unique aspects of the Internet of Things make simple application of the FIPPs a challenge. All new products and services using personal data – whether part of the Internet of Things or otherwise -- raise privacy concerns. For example, location based services raise a host of privacy concerns, and responsible businesses take appropriate steps to inform consumers about data use practices. With the Internet of Things, businesses should have the flexibility to inform consumers in a way that makes sense and to get appropriate consents.

---

[12] Bruce Schneier, *Will Giving the Internet Eyes and Ears Mean the End of Privacy?*, Guardian (May 16, 2013), http://www.guardian.co.uk/technology/2013/may/16/internet-of-things-privacy-google.

[13] *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).

[14] 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.

[15] *See* Evans, *supra* note 8, at 9.

When dealing with technologies that rely on multiple and continuous data inputs, often in circumstances where the consumer is not interacting with a screen and not in a position to make choices, one commentator has asked (and observed):

- How will the principles of notice and choice apply?
- What does transparency mean and what is the right level?
- The challenges of providing access are especially pronounced if there is not a direct interaction with a particular device.
- How do we incorporate privacy by design into the initial design and manufacturing phase to consider/alleviate many of the privacy issues that connected devices might present?
- Can industry self-regulation and the FIPPs work for the [Internet of Things] to form the foundation of global privacy laws and regulations?[16]

One high-level answer to those concerns: 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. Devices could, for example, provide notice of data collection through visual, auditory or tactile cues.

The development of flexible consent mechanisms also should be encouraged. Consent could be obtained in a variety of ways, including consumer profile management portals. In many cases, user interface designs that help communicate to users that an interaction is "smart" may be more effective than traditional consent models.

Companies may be most effective at helping users understand data collection when they help consumers access and use, in some manner, the data that the companies have collected.[17] Examples of this could include allowing consumer apps to access the data as permitted by the end users, providing tools that allow users to add or tailor data to more effectively customize

[16] Rob van Kranenburg et al., *The Internet of Things* (2011), *available at* http://berlinsymposium.org/sites/berlinsymposium.org/files/paper_iot-new_covertext.pdf (paper prepared for the First Berlin Symposium on Internet and Society); *see also* Winter *supra* note 13.

[17] *See* Kranenburg et al., *supra* note 16; Natasha Singer, *If My Data Is an Open Book, Why Can't I Read It?*, NY Times (May 26, 2013), http://www.nytimes.com/2013/05/26/technology/for-consumers-an-open-data-society-is-a-misnomer.html?ref=natashasinger&_r=0.

data, and other methods that help "featurize" data in ways that provide consumer benefits. If companies "share the wealth" of data that they collect, this will provide consumers with an understanding and awareness of the fact that data is being collected and used by companies with whom consumers interact via sensors, and consumers may begin to appreciate the benefits that the Internet of Things can offer. Simply sharing the data that has been collected with consumers will go a long way to demystify what is happening.

Louis Brandeis, who together with Samuel Warren "invented" the legal right to privacy in1890, also wrote that "[s]unlight is said to be the best of disinfectants."[18] If the existence and uses of databases were visible to the public and organizations were required to disclose the basis of their reasoning when engaging in data processing operations that impact individuals' lives, organizations would be more likely to avoid unethical or socially unacceptable uses of data.

On the issue of security, the Internet of Things will not be able to achieve its full potential unless administrative and technical measures are in place to protect against authorized access or disclosure of data collected by connected devices. There are concerns that a network of connected devices could introduce or accelerate unexpected, catastrophic failures known as "black swan events", such as the entire power grid shutting down.[19] And it is understandable that people fear the possibility of hackers accessing and controlling their household devices or vehicles.

The Internet of Things presents challenges. Meeting these challenges will require the establishment of standards and practices that are tailored to meet them without depriving the public of the benefits that the Internet of Things can offer. As European stakeholders have cautioned, any "one-size-fits-all" approach would be inadvisable and likely counterproductive within the context of connected devices: "Any guideline or standard provided in this field should take . . . diversity into consideration and hence be context based and flexible."[20]

---

[18] Louis D. Brandeis, *Other People's Money and How the Bankers Use It* 92 (1914), *available at* http://www.law.louisville.edu/library/collections/brandeis/node/196.

[19] Andrew Rose, *The Internet of Things Has Arrived -- And So Have Massive Security Issues*, Wired (Jan 11, 2013), http://www.wired.com/opinion/2013/01/securing-the-internet-of-things/; Laurence Cruz, *Securing the Internet of Things*, CISCO (Mar. 24, 2013), http://newsroom.cisco.com/feature-content?type=webcontent&articleId=1158640.

[20] Report on the Public Consultation of IoT Governance, European Commission, Directorate-General for Communications Networks, Content and Technology 5-6 (2013).

IV. Lessons from the 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. 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.

In a report entitled *A Policy Framework for the 21st Century Grid*, the White House recognized that "[s]mart grid technologies and programs represent an evolution in how our electricity system operates. . . . [And] this transition offers significant promise for utilities, innovators, consumers, and society at large."[21] 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.[22] 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*

[21] Executive Office of the President, National Science and Technology Council, *A Policy Framework for the 21st Century Grid: Enabling Our Secure Energy Future*, (June 13, 2011), *available at* http://www.whitehouse.gov/sites/default/files/microsites/ostp/nstc-smart-grid-june2011.pdf.

[22] Will McNamara, West Monroe Partners, *Opt-Out Programs May Impact AMI Business Case* (July 2012), http://www.westmonroepartners.com/en/insights/newsletters/west-news-energy-and-utilities-july-2012/opt-out-programs-may-impact-ami-business-case.

Electricity Conservation."[23] 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."[24] 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 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.[25]

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.

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.[26] FPF supports creative approaches to the challenges raised by the smart grid.

---

[23] *Smart Privacy for the Smart Grid, supra* note 3.
[24] *Id.* at 9.
[25] *Id.* at 10-11.
[26] *See Comments of the Future of Privacy Forum on the Proposed Decision Adopting Rules to Protect the Privacy and Security of the Electricity Usage Data of the Customers of Pacific Gas and Electric Company, Southern California Edison Company, and San Diego Gas & Electric Company* (June 2, 2011), *available at* http://www.futureofprivacy.org/wp-content/uploads/2011/06/FPF_Cal_PUC_Smar_%20Grid_Comments.pdf; *Comments of the Future of Privacy Forum in the Matter of the Proposed Rules Relating to Smart Grid Data Privacy for Electric Utilities, 4 Code of Colorado Regulations 723-3* (Mar. 24, 2011), *available at* https://www.dora.state.co.us/pls/efi/efi_p2_v2_demo.show_document?p_dms_document_id=102498;

To that end, FPF developed a first-of-its-kind privacy seal program for companies providing services to consumers that rely on energy data.[27] Powered by TRUSTe,[28] a leading data privacy management organization, the seal program provides privacy guidelines that govern the collection, storage, use and disclosure of consumer energy data. The guidelines promote user control and rely upon the FTC's FIPPs.[29]

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'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.

While the seal provides a degree of flexibility, it also supports and reinforces traditional privacy principles. For example, it requires that companies notify consumers and obtain their consent prior to when the companies contemplate sharing previously collected information in new ways. Data minimization is encouraged by requiring that companies only collect and retain information for which they have a specific business purpose. The seal encourages businesses to provide meaningful transparency through concise, accessible and reasonably comprehensible privacy policies that explain what types of data will be used, how that data will be used and provide options to consumers to control their data. The seal provides a degree of oversight and assurance

---

Comments of the Future of Privacy Forum in the Matter of a Commission Inquiry into Privacy Policies of Rate-Regulated Energy Utilities, (Jan. 29, 2013).

[27] For more information, see the Future of Privacy Forum's Smart Grid resource page at http://www.futureofprivacy.org/issues/smart-grid/.

[28] *TRUSTed Smart Grid*, Truste, http://www.truste.com/products-and-services/enterprise-privacy/TRUSTed-smart-grid (last visited May 31, 2013).

[29] *Fair Information Practice Principles*, Fed. Trade Comm'n, http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last modified Nov. 23, 2012).

that is needed to ensure customer trust, offers an additional layer of oversight to utility regulators and helps utilities provide their customers with the information needed to make sophisticated privacy decisions. A privacy seal program is a first step to ensuring that consumers are provided with the timely information needed to understand how their energy consumption data is collected and used.

Providing organizations and regulators with the tools necessary to promote customer trust is essential both for the development of smart grid technologies and the broader Internet of Things. 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. Ensuring that consumers understand that they will benefit from these innovations is important lest they feel that customer control has been sacrificed for corporate gain.[30] In the case of the smart grid, FPF saw an opportunity to align consumer control over their energy usage with control over their personal information, and this approach could be valuable across the entirety of the Internet of Things.

V. Connected Cars and Attention to the Privacy and Security Issues

Connected cars also serve as a useful example of the challenges and benefits that arise from the implementation of connected devices in the Internet of Things. Connected vehicles today provide significant safety, security and convenience functions.

In the event of an accident or carjacking, connected car technologies can dispatch 911 services. Parents can monitor the location and speed of teen drivers to ensure their safety. Owners of certain connected cars can warm or cool their parked vehicles remotely before getting into them.

Future developments will allow a vehicle to monitor and process conditions inside and outside the vehicle to make the driver and passengers safer, and to make trips easier and more efficient. For example, if a vehicle's connected system indicates a malfunction or other hazardous situation, it will be able to direct the driver to a nearby service center or even disable the vehicle.

[30] *See generally* Winter, *supra* note 13.

Gone will be the days of the ambiguous and often mistaken "Check Engine" dashboard light or worse, an unexpected dangerous mechanical failure. If the connected vehicle determines through analysis of driving patterns that the driver is lost, the vehicle will assist with directions. Vehicle manufacturers should be able to use information collected from vehicles to improve the design and performance of vehicles. City planners and departments of transportation should be able to use aggregate driving information to optimize traffic flows and identify roads in need of repair.

According to one survey, the growth of embedded in-car telematics will ensure that connected cars make up over 5% of connected devices by 2025, compared with just 0.1% today.[31] By 2025, over 600 million connected cars could be on roads worldwide.[32] This explosive growth in connected cars will likely increase safety on our roadways, improve our commutes and make driving a much more enjoyable experience. Without adequate guidelines, however, particularly those that address privacy and security issues, these benefits may not be realized.[33]

Vehicles are becoming "connected" in a variety of different ways. Smartphones are often an integral component in providing cars with access to an outside cellular network,[34] but embedded telematics and external devices that are brought into the car are increasingly being used to enable vehicle connectivity. This connectivity provides easy-access to our day-to-day driving habits and the operational condition of our cars, which promises a variety of benefits to public authorities, car manufacturers, insurers, content and service providers, and ultimately, drivers themselves.

A. Connected-Car Services

Navigation services in vehicles are nothing new, and in their basic form involve "one-way" communication, not really implicating the concept of "connected cars". Many navigation systems operate without Internet connectivity by relying on onboard systems that calculate location information based on GPS signals and using onboard mapping and navigation systems. There are effectively no privacy issues with the provision of these services. Likewise,

[31] SBD & GMA, *2025 Every Car Connected: Forecasting the Growth and Opportunity* 15 (2012), *available at* http://www.gsma.com/connectedliving/wp-content/uploads/2012/03/gsma2025everycarconnected.pdf.
[32] *Id.* at 14.
[33] *See* Evans, *supra* note 8, at 9.
[34] *See generally* Rani Molla & Kevin Fitchard, *The Connected Car of the Future*, GIGAOM (Feb. 6, 2013), http://gigaom.com/2013/02/06/the-connected-car-of-the-future-infographic/.

sophisticated "infotainment" systems, with one-way flows of data, are not privacy sensitive. When navigation systems are connected to other systems, however, additional features and efficiencies can be offered. Navigation can be enhanced by the integration of Internet search services. Maps can more readily be updated. Directions can be tailored to avoid heavy traffic.

Connected vehicles can also serve to entertain and provide communications services for drivers and passengers. Passengers can use hotspots within vehicles to access the Internet via their mobile devices. Drivers and passengers alike can avail themselves of in-car apps that provide information about weather, fuel prices, parking information, travel updates and more. Vehicle displays can also allow individuals to access their favorite apps, such as streaming music services, social media platforms and news feeds.

Vehicle diagnostics services are an essential feature of many connected vehicle offerings. By analyzing data collected from vehicles against a set of historical data, providers of connected-car services can warn drivers of potential dangers, such as brake failures. Drivers can receive notice that their vehicles require service and can receive directions to the nearest service station. Vehicle-to-vehicle communications allow vehicles to be "aware" of what is happening with surrounding vehicles. Vehicle monitoring services allow owners to receive alerts when vehicles travel outside certain areas or exceed set speed parameters and facilitate the recovery of stolen vehicles. Remote vehicle control services allow vehicles to be disabled or slowed down when needed.

B. Benefits of Connected-Car Services

The services that connected vehicles offer provide a number of benefits. According to a 2011 report published by Cisco Internet Business Solutions Group, connected vehicles could create an annual benefit pool of $1,400 for each connected passenger vehicle.[35] These economic benefits, which will flow to consumers as well as businesses, are predicted to flow from the consolidation of communications systems, such as audio services, toll passes and parking passes; reduced service costs; less time stuck in traffic; accident reductions; reduced emissions; and other

[35] Andreas Mai & Dirk Schlesinger, *A Business Case for Connecting Vehicles: Executive Summary* 4 (2011), *available at* http://www.cisco.com/web/about/ac79/docs/mfg/Connected-Vehicles_Exec_Summary.pdf.

benefits. These benefits are predicted to accrue to vehicle manufacturers, service providers, individual drivers, the government and society at large.[36]

Connected vehicles provide a range of personal safety benefits. A connected vehicle can alert emergency responders that an accident has occurred and provide information about where emergency or roadside assistance services need to be dispatched. A connected vehicle can warn drivers of potential vehicle malfunctions and offer location-based warnings regarding weather or road conditions. The information collected from vehicle-to-vehicle communications can be used to prevent accidents by slowing down or otherwise altering a vehicle's operations when the network of information indicates that an accident is likely to occur nearby. Lastly, connected vehicles can promote the safety of teen drivers by allowing parents to monitor where and how their children are driving. Snapshot, offered by Progressive Insurance, for instance, allows vehicle owners to receive reports about drivers' braking habits, how far the car is driven and whether the car is driven at night.[37]

Connected vehicles can also contribute to public safety. When law enforcement receives notice that a car has been stolen, monitoring services can allow them to locate and recover the vehicle. The suspects in the Boston Marathon bombing were tracked and located through such a monitoring service.[38] If the vehicle is equipped with remote disabling or throttle reduction services, the vehicle can be brought to a stop or slowed down without having to engage in a dangerous, high-speed pursuit. When emergency vehicles are equipped with navigation systems enhanced with up-to-date traffic information obtained over the Internet, those emergency vehicles can be dispatched to emergency locations more efficiently. If the driver of a connected vehicle alerts emergency service providers to a roadside incident, the vehicle's location information can inform the emergency providers of where the incident is. The increasing number of vehicles utilizing electric power sources increases the risks of battery fires. Connected vehicles can allow telematics systems to monitor the status of those batteries during day-to-day operations and after accidents to determine whether there is a risk of a battery fire. If

[36] *Id.* at 4-11.
[37] *How Snapshot Works*, Progressive Insurance, http://www.progressive.com/auto/snapshot-how-it-works/ (last visited May 31, 2013).
[38] *Boston Police: Marathon Bombings Suspect 'in Custody'*, CNN (Apr. 20, 2013), http://edition.cnn.com/2013/04/19/us/boston-area-violence.

such a risk presents itself, a connected vehicle can tell emergency responders where to go to address the incident.

Consumer convenience is yet another benefit offered by connected vehicles. Remote monitoring services allow drivers to observe their vehicles' statuses without having to get inside their cars. Drivers can tell whether they need to engage the parking brake, get fuel, inflate their vehicles' tires or get an oil change by accessing a web portal or mobile app. They can also monitor and control whether the doors are locked or the windows or doors are open. To locate a vehicle in a parking lot or call attention to a vehicle's location, drivers can remotely activate their vehicles' horn and lights.[39] Connected vehicles are also able to receive vehicle diagnostic reports and warnings about needed services.

Location-based services and vehicle monitoring can also greatly improve the consumer experience. Navigation and communication systems can provide drivers with location-based information (relating to current or requested locations) about weather, travel information, fuel prices, points of interest, parking availability, notable events and traffic. Drivers can receive location-based offers from mechanics, restaurants, retailers and more. Insurers can offer discounts to drivers who manifest safe-driving habits.

The communications and infotainment systems of connected vehicles provide drivers and passengers with a host of conveniences. A broad range of audio entertainment can be provided via apps and other services. Passengers can access movies, games and other entertainment by using embedded displays or mobile devices connected to the vehicle's Wi-Fi hot spot. Vehicle occupants can use a variety of communications channels, including phone, SMS text messages, emails and social media. Last, vehicle occupants can communicate with devices at home or at the office. From inside the vehicle, occupants could monitor or control household security systems, garage doors, appliances, thermostats and lights.

Connected car technologies can also have a positive effect on the environment. Traffic congestion can be reduced by using information collected from vehicles to manage traffic and optimize road networks. Vehicles can intelligently adjust driving speeds to boost fuel efficiency.

[39] Chris Woodyard, *Who Needs a Key? IPhone App Unlocks and Starts Car*, USA Today (Oct. 16, 2009), *available at* http://readwrite.com/2013/03/14/how-connected-cars-might-actually-make-driving-better.

Cisco estimates that the widespread implementation of connected vehicles could reduce carbon dioxide emissions by 3%.[40] By utilizing vehicle-to-vehicle communications to reduce accidents and vehicle monitoring to identify and prevent potential malfunctions, connected-car technologies would likely reduce a wealth of hazardous materials.

Businesses will also obtain benefits and develop innovative business models by utilizing connected-car technologies. Insurers are already offering safe-driving discounts based on driving behavior,[41] and financing companies may be able to offer preferential terms to consumers with low risk profiles.[42]

C. Privacy Issues

Providing these benefits, however, involves collecting personal information, which many drivers may view as extremely sensitive. Drivers often see their cars as an extension of their homes. As vehicles become more able to collect information about the actions and location of drivers, the privacy risks to consider are obvious.

Many of the potential services being offered by connected-car technologies are similar to the challenges facing the mobile app ecosystem as a whole. Fortunately, car manufacturers offering connected car technologies, as well as the intermediaries proving the technologies and communications technologies have shown a keen awareness of their privacy and security obligations to consumers. FPF recently has convened a working group of companies involved in providing connected car services to help identify and discuss the emerging issues in this area. By sharing best practices and collaborating on industry wide issues, we and companies involved hope to be in a position to help advance responsible policies. FPF hopes this will follow the smart grid model and that will be able to establish best practices that protect consumers and at the same time are flexible enough to encourage innovation.

---

[40] Frederic Paul, *How Connected Cars Might Actually Make Driving Better*, ReadWrite (Mar. 14, 2013), http://readwrite.com/2013/03/14/how-connected-cars-might-actually-make-driving-better.

[41] Progressive Insurance, *supra* note 37.

[42] Telematics providers offering driver profiles for purposes of credit decisioning would, of course, have to ensure that they complied with their obligations under the Fair Credit Reporting Act, 15 U.S.C. §§ 1681 et seq.

VI. The Development of Smart Stores

As consumers have flocked to ecommerce, traditional retailers have begun to look to new technologies to transform the future of shopping. Sensors to combat shoplifting or track inventory, smart mirrors that show consumers what clothing looks like on them without trying it on, location tracking tools that provide analytics about the movements of frequent shoppers or the waiting times at checkout lines, interactive mannequins, smart scanners, geo-fenced coupons and digital signage are just a few of the many innovations making their way into stores.[43] Most of these technologies significantly enhance the in-store consumer experience, but many of them rely on data that will need to be handled in a trustworthy manner to ensure consumer acceptance.

Some of the smart store technologies of particular interest to retailers leverage the interaction of store Wi-Fi networks and mobile phones.[44] Stores can learn how long consumers are waiting in line to check out and can understand how many consumers are repeat shoppers or which window displays are successful at bringing consumers into the store or to a register.[45] In many ways, retailers are seeking to match the advantage that online retailers have gained by using cookies to track how users navigate their Web sites. But industry standards do not yet exist that can guide retailers about the best ways to inform consumers about these practices, how to give consumers choices over when they can be identified and when they are anonymous or how to decline to participate in this type of tracking.

FPF is working with a number of stakeholders interested in ensuring that smart stores are able to use new technologies to better serve consumers while ensuring responsible uses of data. We look forward to sharing further details as our work progresses.

VII. Conclusion

The upcoming FTC Workshop on privacy and security in the Internet of Things promises to provide an excellent opportunity for exploring the many issues involved in protecting individuals

---

[43] Ashley Lutz & Alaina McConnell, *12 Sneaky Ways that Big Retailers Track Your Every Move*, Business Insider (Jan. 1, 2013), http://www.businessinsider.com/retail-tracking-2012-12?op=1.

[44] Steve Henn, *To Keep Customers, Brick-and-Mortar Stores Look to Smartphones*, NPR All Tech Considered (Mar. 27, 2012), http://www.npr.org/blogs/alltechconsidered/2012/03/27/149463201/to-keep-customers-brick-and-mortar-stores-look-to-smartphones.

[45] *See, e.g.*, *Euclid Analytics, How It Works*, Euclid Analytics, http://euclidanalytics.com/product/how/ (last visited May 31, 2013).

while at the same time promoting innovation and benefits from advances in technology. The Future of Privacy Forum looks forward to participating, and hopes these Comments contribute to the exploration of the issues.

Respectfully submitted,

Jules Polonetsky

Co-Chair and Director

Christopher Wolf

Founder and Co-Chair

FUTURE OF PRIVACY FORUM

919 18th Street NW

Washington, DC 200036

www.futureofprivacy.org

May 31, 2013