9 January 2014

TO: Federal Trade Commission (FTC)

FROM: Pedro Pavon, Esq | CIPP/US | | Carlton Fields Jorden Burt 100 S.E. 2nd Street, Suite 4200 Miami, FL 33131

RE: Public Comments on the Internet of Things Workshop

On 19 November 2013, the FTC held a public workshop titled "**Internet of Things - Privacy and Security in a Connected World".** On its website, the FTC says the workshop was intended "to explore consumer privacy and security issues posed by the growing connectivity of devices."

Devices such as refrigerators, cars, and even coffee makers, are becoming "smart," and increasingly connected to the Internet. This phenomenon is known as "The Internet of Things." Connected devices collect and transmit information about their use and the way consumers interact with them. This information is used by manufacturers and third parties to improve technology, provide add-on services, and market new products and services.

With all the new data about consumer habits, behavior, and personal preferences being created and transmitted by Internet-connected devices, privacy protection must become a principal consideration in determining how this new data can be used. Misuse of this data can present significant risks. For instance, analysis of data gathered from the "Internet of Things" ecosystem (meaning data collected from different devices and analyzed collectively) may reveal private or protected data about consumers, such as information related to health care or education, which is generally protected by law. Also, data collected by the "Internet of Things" may create unexpected dangers, like alerting would-be thieves about when a consumer is home or when someone is most likely to have extra money or valuables around.

On 11 December 2013, the FTC requested public comment on its Internet of Things Workshop. The FTC provided 15 questions as a suggested framework for the public to provide feedback. The following is a brief response to each question intended to further the understanding of the issue presented. The responses are my own, in my capacity as a privacy law expert, advocate, and consumer, and should not be construed to represent the views of my employer or any of its clients.

How can consumers benefit from the Internet of Things?

There are countless benefits that arise from the proliferation of Internet-connected everyday devices. With interconnectivity and data sharing, consumers can benefit from greater reliability and efficiency from their devices and appliances. Imagine a thermostat you can control remotely to adjust the temperature of your home when you are on vacation. Now imagine unlocking your front door at home from the office so your child, who forgot his keys, can get into the house. These are just two examples of the infinite ways that the Internet of Things will improve consumer quality of life and safety.

Another benefit of the Internet of Things will be the "datafication" of everyday activities. Datafication means using Big Data to track and analyze new large data sets created by all of the devices around you. This will lead to a greater understanding of how we live our everyday lives and will help identify ways to improve our surroundings and make mundane activities—like making coffee—more efficient. Imagine having a coffee maker that "knows" when you are home and automatically brews coffee at a certain time each day. Imagine your refrigerator can alert you (or your grocer) when you are running low on milk so you can pick it up on your way home or have it delivered automatically. All of these possibilities become a reality when devices around us become "smart," work together, and share information to improve the way they meet our needs. Efficiency, reliability, and process are the true promises of Big Data and the Internet of Things.

What are the unique privacy and security concerns and solutions associated with the Internet of Things?

The Internet of Things's great promise is accompanied by difficult challenges regarding datafication's impact on consumer privacy and security. The most significant privacy concern associated with the Internet of Things will relate to how all the data generated from devices is collected, analyzed, and used. One of the biggest benefits of Big Data also produces its most challenging privacy concern: you don't know what you are going to discover until after the data has been analyzed. Seemingly unrelated data points, when analyzed at the scale of Big Data, can reveal embarrassing or private facts about people.

For example, let's consider GPS tracking. On its face, GPS seems pretty straightforward. A device with GPS tracking collects and transmits location data and sends it to a central hub. That central hub then uses the data to provide benefits such as recovering a lost device or getting directions to a restaurant. Over time, more and more data points (in this case, places where the device is located) are collected, and if analyzed in the proper context, using the right algorithms, can reveal much more than plain location data. GPS data, collected and analyzed over time, reveals trends, behavioral information, location preferences, lifestyle choices, and much more. If this data were made public or fell into the wrong hands, it could be used to blackmail or embarrass someone who has chosen

to keep certain parts of her life secret or private. Also, if law enforcement has access to this data it could potentially place innocent people under "GPS surveillance" simply because that's easier than conducting investigative work. The likelihood that a consumer will consider all of these possibilities when prompted to enable the GPS location tracking option on her phone or car are very, very low. The likelihood becomes zero if the GPS option is on automatically from the get-go.

The Internet of Things presents a variety of other privacy problems as well. Just how much do you reveal about yourself for your coffee maker to make your coffee on time, each morning just the way you like it? Do you reveal what time you wake up each morning? Or the days of the week you work and those on which you don't? Do you reveal how many people drink coffee with you? Or how long it takes you to get ready in the morning? The answer to each of these questions is "yes." All of this new information about you can be derived from how you drink your coffee. But when your coffee maker, refrigerator, cellphone, car, thermostat, house alarm, and TV all collect data about you each morning for twenty years, what could that reveal? Could it reveal an accurate picture of who you are, what you like, and how you behave? Who should have access to that data? How should they be allowed to use it? What say do you, the consumer, have in all of this? Is consent enough when the consumer can't possibly understand, and no one can predict, what the data will reveal in five or ten years?

As the Internet of Things proliferates and more devices come online, safeguards and protections will need to be implemented to protect consumers from inadvertent disclosures of private information. The cost of convenience and innovation cannot be the total annihilation of privacy—especially in the home.

Security also becomes a concern when all the devices around you are tracking you and collecting data about you around the clock. For example, if criminals were to gain access to your data profile[1] they would be able to plot their crimes with dangerous precision. Imagine robbers who know exactly what you do every day, and when and where you do it. If they wanted to break into your home, they'd just check the data and commit the robbery when the data shows you are never home. If someone wanted to harm or rob you, they'd check the data and be able to see that you jog alone every night in the park, or hike alone in the mountains once a month, and plan accordingly.

With all your devices online, hackers could also do a lot of damage. A malicious hacker could potentially hack your home and cause havoc. As horrible as that sounds, a hacker, thinking on a grand enough scale, could hack into your home alarm company's control

[1] A data profile is the overall picture of who a consumer "is" as understood by the devices she uses. Depending on how a consumer interacts with her devices, and which devices she interacts with, her data profile can reveal almost anything about her including when and where she goes every day, who she spends time with, what she does, when she does it, and much more.

center and lock everyone out of their homes, set off the fire alarms, or worse, cut off power or heat to millions of homes at once. The Internet of Things will create lots of new ways for criminals to hurt people. This is why, along with privacy protection, security will be a paramount concern as the Internet of Things becomes a reality.

What existing security technologies and practices could businesses and consumers use to enhance privacy and security in the Internet of Things?

Privacy by design will be a critical component to enhancing privacy protections in the Internet of Things. Protecting privacy must be the default mode of operation in the Internet of Things environment. All systems must be designed to ensure that data is collected and used in ways that do not jeopardize consumers' privacy rights or concerns. Enhancing privacy will strengthen security because as explained above, it is the malicious use of the data collected from the Internet of Things that creates the most danger. The Internet of Things ecosystem must be designed to protect privacy and strengthen security by its very nature. In other words, privacy and security should be a key design component for all devices. The regulatory scheme governing the Internet of Things should not focus on how data is collected. Instead, it should aim to protect consumers by strictly regulating how the data from the Internet of Things is used.

Additionally, other practices can be implemented to enhance privacy and security in the Internet of Things. In *An Updated Privacy Paradigm for the "Internet of Things",* a white paper prepared by the Future of Privacy Forum, authors Christopher Wolf and Jules Polonetsky suggest the following practices to enhance privacy and security:

1. Use anonymized data when practical

2. Respect the context in which personally identifiable information is collected

3. Be transparent about data use (and I would add, collection)

4. Create automated accountability mechanisms

5. Provide individuals with access to Personally Identifiable Information (PII)

What is the role of the Fair Information Practice Principles in the Internet of Things?

The Fair Information Practice Principles (FIPPs) have been heralded as a cutting-edge and comprehensive approach to establishing standards and codes of conduct to enhance and strengthen the privacy and security of data and records. However, in the context of the Internet of Things, FIPPs will have limited application.

Notice and choice, both pillars of the FIPPs framework, will have limited value with devices that lack a user interface. For example, it will be impossible (without some

major innovation) to provide a click-through or in-time consent mechanism via an Internet-connected device such as a traffic sensor or one that is embedded as part of a larger machine or system. Additionally, as the Internet of Things evolves and expands to devices outside the home, new devices will become increasingly "hands-off" or invisible to the data subjects. How can a consumer provide consent to a traffic sensor or cell-phone tracking devices at a shopping mall when she is not even aware of them? Device sharing also becomes problematic in the FIPPs schema because the owner or first user of a device may have received notice and provided consent, but the actual user has not.

However, the challenges described above are not as significant as the constant collection privacy problem. FIPPs were designed for, and work well in, discrete collection environments. In such environments, under the FIPPs model, data subjects are provided advance notice describing the types of data being collected and how the data will be used. Upon review, the data subject can then agree or refuse to accept the terms. But in the Internet of Things, that type of notice and consent becomes not only impracticable, but likely impossible because data subjects will not come into contact with all the devices collecting information about them and, or, the devices will lack the capability to properly provide notice. The beauty and promise of Big Data is that when you collect and analyze massive amounts of seemingly asymmetrical or unrelated data at a large scale, you learn new insights that were always there but were impossible to measure due to a lack of data points or because analysis was occurring at the wrong scale. To collect the vast amounts of data necessary to apply Big Data analytics effectively, devices will have to collect data around the clock, and data transmissions will have to be continuous, or at least very frequent. The problem for privacy and security purposes is that you don't know what the data is going to tell you until you collect and analyze it, and therefore it is impossible to know or predict with any certainty, in advance, how you are going to use the data or what its value will be. In fact, at the point of collection, it is impossible to determine if the data will reveal anything at all.

What steps can companies take (before putting a product or service on the market) to prevent connected devices from becoming targets of, or vectors for, malware or adware?

Encryption will have to be a centerpiece of the Internet of Things ecosystem. All data must be secured and encrypted at the point of collection and remain encrypted until it is destroyed. Companies should also take reasonable steps to anonymize data at the earliest point possible even if it is encrypted. Additionally, companies must take steps to limit the data they collect and destroy data when it is no longer being used. Not every device needs a GPS sensor. Companies should avoid collecting data that they don't intend to use right away. Collecting data for its "future potential" or "possible use" is dangerous and companies should promote a design and innovation culture that rejects the idea of collecting as much as possible and instead focuses on collecting data with pre-determined value. Data retention schedules should be assigned to all data collected

by the Internet of Things and every single data point should have as short a lifespan as permitted by commercial needs and regulatory requirements.

How can companies provide effective notice and choice? If there are circumstances where effective notice and choice aren't possible, what solutions are available to protect consumers?

As explained above, notice and choice are not practicable solutions for the Internet of Things. However, there are other methods available to protect consumers. Focus must shift from how information is collected and shared to how it is used. Limits can be placed on use based on the types of devices doing the collecting. Additionally, data can be anonymized to decrease the risk that the information can be used to target individuals or groups. It is also important that companies take steps to maximize transparency about what types of data they collect, how they use it, and for how long. Consumers should also be given access to PII to correct errors or opt-out of collection altogether.

What new challenges does constant, passive data-collection pose?

Constant and passive data collections create several new challenges. As explained above, constant and passive data collection makes the FIPP framework obsolete in some ways. Additionally, as devices become "hands-off" or invisible to consumers, it will be increasingly difficult (or impossible) to keep track of all the devices collecting data about them simultaneously around the clock. To ask consumers to manage all of the data being collected about them by all the devices around them (some of which they don't even see or know about) is an unrealistic recipe for failure. This approach would also give rise to serious criticism about the value being placed on personal privacy by companies making devices for the Internet of Things ecosystem.

What effect does the Internet of Things have on data de-identification or anonymization?

Companies should take steps to anonymize data sets before they are analyzed, shared, or used for any purpose. Anonymizing data decreases its vulnerability to malicious or unauthorized use. However, because it is difficult to predict what Big Data collection and analysis will reveal once the data is "crunched," it will be impossible to guarantee that anonymized data will remain so and not be de-anonymized. Re-identification after analysis, or when data sets from multiple sources are combined and reviewed together, will be a very real possibility. Companies must therefore assess and address the serious risk of re-identification of the data they collect, analyze and anonymize.

How can privacy and security risks be weighed against potential societal benefits (such as improved health-care decision-making or energy efficiency) for consumers and businesses?

Both companies and consumers will have to weigh the risks involved with the Internet of Things. This balancing test will be especially difficult in the context of the Internet of Things because whenever Big Data analytics is involved, as discussed above, the benefits are not always clear until after the data has been analyzed. You cannot consider what you cannot imagine, and making decisions about risk vs. reward when it comes to the Internet of Things will be very difficult. However, companies can take steps to minimize risk and focus on benefit-driven devices and data collection. For example, at the concept stage, engineers should identify real-world problems that must be solved before endeavoring to design new devices or methods of data collection. One of the biggest tech industry challenges is that entrepreneurs and engineers often design devices and systems in search of a problem to solve. The opposite should always be the rule. All engineering should begin *after* a problem to solve is identified. This will put the risk vs. reward equation in favor of the device and data collection, at least at the early stages.

For consumers, increased awareness and education will be key. Consumers must "get smart" about the Internet of Things and the possibilities and drawbacks of Big Data. Government will play a key role in raising consumer awareness. Just as pharmaceutical companies are required to provide an explanation of the risks associated with their products, companies that make devices for the Internet of Things ecosystem should be required to do the same. Additionally, government must implement an aggressive awareness campaign (similar to those related to tobacco, alcohol, and STDs) to raise awareness of the risks and rewards associated with the Internet of Things.

How can companies update device software for security purposes or patch security vulnerabilities in connected devices, particularly if they do not have an ongoing relationship with the consumer? Do companies have adequate incentives to provide updates or patches over products' lifecycles?

Companies should include privacy and security by design as part of all their Internet of Things devices. Companies could also consider issuing privacy or security recalls similar to the safety recalls related to vehicles or children's products. Without a doubt, companies will have to create innovative ways to fix vulnerabilities. Possible ways to do this include designing systems with centralized control, and giving consumers an incentive to keep their devices up to date.

There are several existing incentives for companies to provide updates and keep their devices secure and up to date. The first is to minimize tort liability. The less control consumers have over Internet of Things Devices, the more liability and exposure companies managing those devices will have. The threat of a class-action suit for knowingly permitting devices that pose a security risk to be "in the wild" will be

significant in the future. Additionally, companies will need to be mindful of the regulatory scrutiny they will face if they fail to manage their devices properly.

How should the FTC encourage innovation in this area while protecting consumers' privacy and the security of their data?

The FTC should, in partnership with stakeholders, work to advance a framework to govern the Internet of Things. The FTC could create guidelines or standards and best practices that promote innovation while protecting consumers. The best way to do this is to engage stakeholder representatives from all sides and collaboratively develop the framework or standards and best practices to avoid surprises or pitfalls.

The FTC should also prosecute bad actors aggressively. Unfair and deceptive practices by companies should be met with swift enforcement. The private sector should work with the FTC to identify bad or negligent actors and fix gaps or vulnerabilities in the Internet of Things ecosystem.

Are new use-restrictions necessary to protect consumers' privacy?

As explained above, data collected via the Internet of Things should be regulated at the point of use. Rules to govern use should be created that allow for new benefits and innovation while simultaneously helping to manage or minimize the risk of harm to consumers. It is important that any restrictions on use be malleable and flexible. Because technology evolves so rapidly, rules in this space need to be able to change quickly to address new risks or take advantage of new benefits. Therefore, laws by states or congress may be too slow and rigid to govern this sector. Agencies like the FTC are much better suited to police the Internet of Things to ensure companies can take advantage of new technologies and that the interests of consumers are being considered at every step.

How could shifting social norms be taken into account?

The problem with considering the shifts in social norms when trying to regulate innovation is that the benefits are typically readily apparent early on and the risks or problems only appear after new technologies have become widely accepted and adopted by consumers. Take social media for example. Facebook had nearly one billion users before the privacy concerns related to social media became front-page news. The same will be true with the Internet of Things. Because of the obvious benefits, consumers will race to buy and adopt wearable devices, sensors, trackers, and other Internet-connected devices before they understand exactly how all these devices will impact their privacy and security. Therefore, social norms can be used as one factor in considering how to regulate the Internet of Things, but should only be a minor one.

How can consumers learn more about the security and privacy of specific products or services?

As explained above, general awareness campaigns by government and the private sector will be necessary. There should be public forums, town halls, and free training and educational tools made available to consumers. Retailers and resellers of Internet of Things devices should also be involved in this process. Trust between consumers, government, and companies will be essential for the Internet of Things to reach its full potential.

For specific products, the burden will be on manufacturers and sellers to educate consumers on specific features and services. When you buy a car, the salesman walks you through every single one of its features, demonstrates how everything works. The same may be necessary for most Internet of Things devices—especially the more complex ones or the "wearables." However, the real challenge will be how to educate consumers on devices they don't see or buy themselves, such as traffic sensors. How do you educate consumers on how they are being tracked by the Internet of Things when they go to the mall, or when they walk or drive down the street and devices in the environment (that they aren't even aware of) are tracking all of their movements?

How can consumers or researchers with insight into vulnerabilities best reach companies?

The easiest way to get a company's attention is with cash. Consumers can weigh in on preferences simply by choosing to buy one device instead of another, or by buying nothing at all. Again, the more complex challenge presents itself when devices they haven't purchased themselves are tracking consumers.

It may be beneficial for the FTC to consider creating an online platform (think Reddit) that allows consumers to visit and engage government and companies directly. Interagency and stakeholder workgroups should be created that include government officials, private companies, subject-matter experts, and consumer groups to ensure that all relevant actors have a voice in shaping the Internet of Things and the future.